MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 4/1983

Anwendbare Algebra
16.1. bis 22.1.1983

Diese erste Tagung über anwendbare Algebra fand unter der Leitung von T. Beth (Erlangen) und H. Lüneburg (Kaiserslautern) statt. Die thematische Spanne der Beiträge war groß, sie reichte von Anwendungen der Algebra innerhalb der Mathematik - insbesondere der Kombinatorik, Komplexitäts- und Darstellungstheorie - bis hin zur Behandlung konkreter Probleme in verschiedenen Bereichen der Technik. In allen Beiträgen spiegelten sich die mannigfachen Wechselwirkungen zwischen neuen Methoden der Algebra und Verfahren der Informatik wider. Fragestellungen der Informatik waren auch der Grund für die Einrichtung von Übersichtsvorträgen, die gemeinsam mit den Teilnehmern der gleichzeitig stattfindenden Tagung über deskriptive Mengenlehre gestaltet wurden.

Besonderer Dank gilt der Leitung des Mathematischen Forschungsinstituts Oberwolfach - vor allem Herrn Professor Barner - für die Unterstützung beim Zustandekommen dieser Tagung. Ebenso muß den Mitarbeitern des Instituts der Dank aller Teilnehmer ausgesprochen werden, da nur durch ihre gute Organisation und freundliche Betreuung jene gute Arbeitsatmosphäre geschaffen werden konnte, die zum Gelingen der Tagung nicht wenig beitrug.

Vortragsauszüge

T. Beth

Applicable Algebra in Signal Processing

Starting with applications in Digital Signal Processing the many methods of Fast Discrete Fourier Transforms are discussed. Considering the Discrete Fourier Transform over Finite Groups as the canonical mapping associated with the Wedderburn-decomposition of the semi-simple Group ring, different very fast DFT-algorithms are derived.

A special transform - ADFT - is presented which performs this task in real time with additive formal operations only.

B. Buchberger

A Critical-Pair/Completion Algorithm for Ideals in $Z[x_1,\ldots,x_n]$

The combined strategy of "critical pairs" and "completion" has been introduced in the author's dissertation 1965 (see aequ. math. 4/3 (1970), 374-383) in order to construct standard bases ("Gröbner-bases") for polynomial ideals over $K[x_1,\ldots,x_n]$. These bases may be used for an algorithmic solution for many fundamental problems in polynomial ideal theory. Improvements of the algorithm have been studied by the author in SIGSAM Bull. 1976 and EUROSAM conference 1979 (Springer LN in Comp. Scie. 72). M. Lauer 76, W. Trinks 77, M. Bergman 78, G. Zacharias 78, S. Schaller 79, J. Guiver 82 have given generalizations of the algorithm for coefficients taken from a ring satisfying certain conditions. However, the algorithm looses its simple structure by some of these generalizations or fairly complicated conditions must be required of the underlying ring. In this talk it is shown how the correctness proof for the algorithm in its original form can be established using only very simple properties of the coefficient ring.

G.E. Collins

The Projection Operation in Cylindrical Algebraic Decomposition

The role of projection in cylindrical algebraic decomposition and the theoretical foundations of projection are discussed. A new theorem (with Scott McCallum, 1983) is presented which effects a large reduction in the size of the projection sets for polynomials in three or more variables. A CAD for Kummer's surface is presented for illustration.

A. Kerber

Applications (to combinatorics) of the representation theory of finite symmetric groups

Two cases were mentioned:

(i) The enumeration of matrices over $\mathbb{N}$ or over $\{0,1\}$ with presecribed row and column sums,

(ii) the question of unimodality of sequences which occur in combinatorial theory of enumeration (e.g. graphs on p points and with $0,1,\ldots,\binom{p}{2}$ edges, the coefficients of the Gaussian polynomials).

For details see the forthcoming paper:
A. Kerber/K.-J. Thürlings: Symmetrieklassen von Funktionen und ihre Abzähltheorie.
Bayreuther Mathematische Schriften (Teil I in print).

E. Köhler

Über die arithmetische Komplexität einiger Produkte

Sei R ein Ring und $a_0,\dots,a_{n-1},b_0,\dots,b_{n-1}$ seien Unbestimmte über R . Ferner sei $\mathbb{Z}_n = \{1,\alpha,\alpha^2,\dots,\alpha^{n-1}\}$. Ist nun $k \in \mathbb{N}$ gegeben, so ist dazu das maximale $x_{k,n} \in \mathbb{N}$ gesucht, für welches gilt:

$$M_{n,k} = n^2 - x_{n,k} \quad \text{und} \quad A_{n,k} \leq n(n-1) + k \cdot x_{n,k} .$$

Hierbei ist $M_{n,k}$:= Anzahl der Multiplikationen und

$A_{n,k}$:= " " Additionen und Subtraktionen

eines Programmes, welches $c_0,\dots,c_{n-1} \in R[a_0,\dots,a_{n-1},b_0,\dots,b_{n-1}] =: R_n$ berechnet mit $\left(\sum_{i=0}^{n-1} a_i\alpha^i\right)\left(\sum_{i=0}^{n-1} b_i\alpha^i\right) = \sum_{i>0}^{n-1} c_i\alpha^i$ im Gruppenring $R_n(\mathbb{Z}_n)$.

Durch explizite Konstruktion einiger Programme wird gezeigt:

$$x_{2,4} = 1 \ , \ x_{3,4} \geq 2 \ , \ x_{4,4} \geq 4 \ , \ x_{5,4} \geq 9 .$$

H.W. Lenstra

Primality testing

Given a large positive integer n , how can one quickly tell whether or not n is a prime number? In this lecture we discuss the theory behind the currently used practical methods to do this. Most methods consist of subjecting n to a collection of tests with the following two properties: (i) if n is prime, then it passes the tests; (ii) conversely, if n passes the tests, then it can be deduced that every divisor r of n is in a certain sense a power of n, the precise sense in which this is true depending on the particular method. From this information one then hopes to be able to conclude that $r = n^0$ and $r = n^1$ are the only divisors of n , so that n is prime. This general description does not apply to the Monte Carlo methods. In the lecture, special attention is paid to tests of an algebraic nature, in

which algorithms related to finite fields play a role. One constructs a ring A that if n is prime is the finite field of order n^t , for a suitable small positive integer t . The tests that one uses consist of checking certain properties of A that are known to hold if n is prime. Conversely, if A has these properties then every divisor of n is congruent to a power of n modulo the largest divisor s of $n^t - 1$ that one is able to factor completely. If s is sufficiently large, e.g. larger than $n^{1/2}$, this enables one to finish the primality test in a straightforward way. The Lucas-Lehmer test for Mersenne numbers $n = 2^m - 1$ can be obtained as a special case, with $t = 2$.

R. Loos

On the Implementation of Abstract Algebra

A survey is given on implementation issues of a large software system for Computer Algebra. Trade offs between the efficiency of primitive list processing and arithmetical operations are described. Some suggestions regarding algebraic software on current technology, in particular a MC 68000 processor, are made.

H. Lüneburg

Uses of Galois fields in cyclotomy

Using the splitting of the n-th cyclotomic polynomial Φ_n into irreducible polynomials over GF(p) , p a prime, and some of the elementary properties of resultants and discriminants, i.e., not using the machinery of algebraic number theory, one can compute or prove: 1) $\mathrm{Res}(\Phi_m, \Phi_n)$. 2) $\mathrm{Dis}(\Phi_n)$. 3) If $\Phi_n(\zeta) = 0$, then $R = \mathbb{Z}[\zeta]$ is a Dedekind domain, i.e., R is the ring of all algebraic integers contained in $\mathbb{Q}[\zeta]$. 4) If p is a prime and if $f_1, \ldots, f_t$ are the pairwise non-associate irreducible factors of Φ_n over GF(p) and if ζ is a root of Φ_n , then $P_i = pR + f_i(\zeta)R$ are the maximal ideals of R containing p . 5) If p does not divide n or if $p = 2$ and $n \equiv 2 \bmod 4$, then $pR = \prod_{i=1}^{t} P_i$. 6) If $n = p^e m$ with $m \not\equiv 0 \bmod p$ and $p^e \geq 3$, then $pR = \prod_{i=1}^{t} P_i^{\varphi(p^e)}$, where φ is Euler's totient function.

C.J. Mitchell

Permutation problems associated with cryptographic devices

Permutations from the set $A(n,k)=\{\alpha \in S_n \mid i^{\alpha} \in \{i,i-1,\ldots,i-k+1\}$ for each $i\}$ are used in time element speech scramblers, and thus $|A(n,k)|$ is of interest. The authors (Henry Beker and the speaker) have produced an algorithm which can be used to evaluate $|A(n,k)|$ for $k \leq 12$ and "reasonable" values of n on a PDP-11 minicomputer.

Previous work on the problem has been done by W.O.J. Moser in Canad. J. Math. 19(1967) 1011-1017 ($k=n-3$) , N. Metropolis et.al. in J.C.T. 7(1969) 291-321 ($k \leq 9$) and E.G. Whitehead, jr. in J. Austral. Math. Soc. (Ser. A) 28 (1979) 369-377 ($k=n-4$) .

Also of interest is the set $B(n,k) = \{\alpha \in A(n,k) \mid i^{\alpha} \neq (i-1)^{\alpha}+1$ for each $i\}$. Much less work has been done on this problem, although the authors have obtained recurrence relations for the cases k=3 and 4 .
In particular the authors would very much like (at least good estimates for) $|A(48,16)|$ and $|B(48,k)|$ for k=8,12 and 16 .

H. Niederreiter

Finite fields and the generation of pseudorandom numbers

Feedback shift registers with arithmetic over finite fields have been used extensively for the purpose of generating pseudorandom digits and uniform pseudorandom numbers. We carry out a theoretical analysis of the statistical properties of output sequences of feedback shift registers, with a view to establishing a priori criteria for the suitability of a given register for pseudorandom digit (or number) generation. T[illegible] methods of transforming pseudorandom digits into pseudorandom numbers in [0,1] are used, namely the normalization method and the digital method.
Effective estimates for the deviation from equidistribution and for the amount of statistical dependence among successors (in the sense of two-sided Kolmogorov tests) are obtained in terms of the least period of the output sequence and a quantity depending on the characteristic polynomial of the register. It is then shown that an appropriately designed register will yield an output sequence behaving very well

with regard to equidistribution and statistical independence of successors. The proofs depend on a principle of quantitative Fourier inversion, relating the Kolmogorov test deviations to the size of character sums over the underlying finte field, and on sharp estimates for these character sums.

H. Pahlings

Computing with Characters of Finite Groups

A computer system "CAS" for handling characters of finite groups has been developed in joined work with J. Neubüser and W. Plesken. The implementation was carried out by M. Ansman, W. Jannißen, and H. Lammers. Some of the facilities of CAS are presented. It is shown, how they can be used for constructing character tables, detecting subgroups, computing Molien series, and finding blocks and decomposition numbers.

W. Plesken

Gitter und unimodulare Gruppen

Gitter sind die von Basen eines Euklidischen Vektorraumes erzeugten abelschen Gruppen. Es werden zwei Algorithmen vorgestellt. Der erste geht aus von einer endlichen Gruppe G , die auf einem Gitter operiert; er bestimmt die G-invarianten Teilgitter von endlichem Index und entscheidet Isomorphie. Der zweite Algorithmus geht von der oben beschriebenen geometrischen Situation aus und berechnet ein Erzeugendensystem der Automorphismengruppe des Gitters. Als Anwendung des ersten Algorithmus wird die Bestimmung der $\mathbb{C}$-irreduziblen maximal endlichen Untergruppen von $Gl_n(\mathbb{Z})$ für $5 \leq n \leq 9$ diskutiert (Plesken, Pohrt 77,80) und die Bravaisklassifikation der 5-dimensionalen Gitter (Plesken 81). Der zweite Algorithmus wird zur Verifikation einer Vermutung von J. Thompson über geschichtete ganzzahlige Gitter, die von Vektoren kürzester Länge m erzeugt werden, für den Fall $m = 3$ benutzt (Plesken, Pohrt 82) und zur Bestimmung der maximal endlichen irreduziblen Untergruppen von $Gl_p(\mathbb{Z})$, p Primzahl ≤ 19 .

H.P. Rieß

The Miracle Octad Generator - materialized

There was presented a MOG - as it was suggested by Sloane and Conway - and a decoding algorithm for the extended binary Golay code by J.M. Goethals. There was also demonstrated a little machine which is able to display the designs

$S(5,8,24)$, $S(5,6,12)$, $S_2(3,6,12)$, $S(2,5,21)$, $S(2,4,16)$, $S(2,3,9)$

and to decode the Golay code.

V. Strassen

Some results in algebraic complexity theory

A survey is given on the complexity of associative algebras and on the degree method.

(Berichterstatter: H.P. Rieß)

Tagungsteilnehmer

Dr. T. Beth
Institut für Mathematische
Maschinen und Datenverarb. I
Universität Erlangen-Nürnberg
Martensstraße 3
8520 Erlangen

Prof. Dr. B. Buchberger
Institut für Mathematik
Universität Linz
A-4040 Linz
Austria

Dr. M. Clausen
Mathematik II
Universität Bayreuth
Postfach 3008
8580 Bayreuth

Prof. Dr. G.E. Collins
Computer Sciences Dept.
University of Wisconsin
1210 W. Dayton Street
Madison, Wisconsin 53706
U.S.A.

Dipl. Inf. Walter Fumy
Institut für Mathematische
Maschinen und Datenverarb. I
Universität Erlangen-Nürnberg
Martensstr. 3
8520 Erlangen

Dipl. Math. H. Gerlach
FB Mathematik
Universität Kaiserslautern
Erwin-Schrödinger-Str.
6750 Kaiserslautern

Dr. T. Grundhöfer
Mathematisches Institut
Universität Tübingen
Auf der Morgenstelle 10
7400 Tübingen

Dipl. Inf. M. Hain
FB Mathematik
Universität Kaiserslautern
Erwin-Schrödinger-Str.
6750 Kaiserslautern

Prof. Dr. D. Jungnickel
Mathematisches Institut
Universität Gießen
Arndtstr. 2
6300 Gießen

Prof. Dr. O.H. Kegel
Mathematisches Institut
Universität Freiburg
Albertstr. 23b
7800 Freiburg i.Br.

Prof. Dr. A. Kerber
Mathematik II
Universität Bayreuth
Postfach 3008
8580 Bayreuth

Prof. Dr. E. Köhler
Mathematisches Seminar
der Universität Hamburg
Bundesstr. 55
2000 Hamburg 13

Prof. Dr. H.W. Lenstra jr.
Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
NL-1018-WB Amsterdam
Niederlande

Prof. Dr. R. Loos
Fakultät für Informatik
Universität Karlsruhe
Postfach 6380
7500 Karlsruhe 1

Prof. Dr. H. Lüneburg
FB Mathematik
Universität Kaiserslautern
Erwin-Schrödinger-Str.
6750 Kaiserslautern

Dr. C.J. Mitchell
Racal-Comsec Limited
Milford Industrial Estate
Tollgate Road
Salisbury Wiltshire SP1 2JG
England

Prof. Dr. H. Niederreiter
Mathematisches Institut
Öster. Akademie d. Wissenschaft.
Dr.-Ignaz-Seipel-Platz 2
A-1010 Wien
Österreich

Prof. Dr. H. Pahlings
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
5100 Aachen

Priv.-Doz. Dr. W. Plesken
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
5100 Aachen

H.P. Rieß
Institut für Mathematische
Maschinen und Datenverarb. I
Universität Erlangen-Nürnberg
Martensstraße 3
8520 Erlangen

Prof. Dr. V. Strassen
Institut für Angewandte
Mathematik
Universität Zürich
Rämistr. 74
8008 Zürich
Schweiz

Dr. V. Strehl
Institut für Mathematische
Maschinen und Datenverarb. I
Universität Erlangen-Nürnberg
Martensstraße 3
8520 Erlangen