MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 8/1993

Applicable Algebra

14. bis 20. Februar 1993

The 1993 meeting dedicated to the area of Applicable Algebra was the third on this topic held at Oberwolfach after the first conference " Anwendbare Algebra " in January 1983 and the second conference " Applicable Algebra " in January 1989.

This year's conference was planned by the three organizers Thomas Beth (Karlsruhe), Bruno Buchberger (Linz) and Heinz Lüneburg (Kaiserslautern) to address areas from Algebra and its applications, like Coding Theory, Cryptography, design of computer algebra systems, digital signal processing, robot programming, geometrical modelling and abstract data types. The emphasis was on such applications which require solution methods from typical algebraic areas such as: Arithmetics in real, complex, p-adic and finite fields, discrete mathematics, number theory, group theory, representation theory, algebraic logic and algebraic geometry.

The positive atmosphere of Mathematisches Forschungsinstitut Oberwolfach supported by the well-known hospitality of all stuff and the dedication of Professor Dr. Barner, the director of the institute, has made it possible to conclude this conference with an extremely positive feeling by all participants.

Vortragsauszüge

R. M. Beals.
Las Vegas Algorithms for Matrix Groups.

We consider the following type of problem: given a finite group G of matrices by a list of generators, determine the order of G, decide membership in G, find Sylow subgroups and composition factors of G.

For the case of finite matrix groups over the rationals (and over algebraic number fields) we solve all these problems in polynomial time by randomized algorithms. The algorithms are of the "Las Vegas" type: they use randomization along the way but the output is certified correct. (There is a negligible chance that the output will be an honest failure report.)

These results considerably extend previous results on permutation group computations into the potentially more significant domain of matrix groups. Such an extension has until recently been considered intractable.

In the case of finite characteristic one faces problems like the discrete logarithm and factoring integers even in the 1-dimensional case. With some caveats, our results extend to this case as well and give further evidence to the conjecture that these number theoretical obstacles are the only obstacles to much more efficient handling of matrix groups. Although we have not implemented the algorithms yet, our results seem to have the potential of considerably increasing the parameters of matrix groups that can be handled by current computers (dimension, order of field of definition). (Existing packages represent matrix groups as permutation groups, causing an immediate fatal blowup in the input size unless the parameters of the group are very small.)

Our algorithms built on a variety of recent randomization techniques, including refined random walk techniques, as well as a statistical analysis of various classes of finite simple groups. The classification of the finite simple groups is extensively used, even when the objective is merely to determine the order of the given matrix group.

This is joint work with L. Babai.

P. CAMION.

Towards a Better Complexity Algorithm to Compute the Minimal Polynomial of a Matrix.

We are given any matrix A of size n×n over a field K together with the factors in K[x] of its characteristic polynomial $\chi_A(x) = f_1(x)^{r_1} \ldots f_k(x)^{r_k}$. Then two algorithms are given to compute the minimal polynomial $\mu_A(x) = f_1(x)^{s_1} \ldots f_k(x)^{s_k}$. of A.

Both algorithms pass through a block-diagonal form of the matrix. This is done by successive evaluations of polynomials to matrices of decreasing sizes, the two first ones being $\prod_{j\in J} f_j(A)^{r_j}$, $\prod_{j\in \tilde{J}} f_j(A)^{r_j}$, for a well chosen partition of [1,k] into J and [1,k]-J. A lemma leads to the successive refinements of the partition. For the whole computation the complexity is shown to be the one of evaluating a polynomial of degree n to matrix A. For the first algorithm it is $O(n^3\sqrt{n})$ and for the second it is $O(n^3 c(n))$ where c(n) is the expected number of factors $r_1 + r_2 + \ldots + r_k$ of the characteristic polynomial.

For the first algorithm, let $U(A) = u_0 I + u_1 A + u_2 A^2 + \ldots + u_t A^t$ to be evaluated, where, for simplicity, $t = 2^{2k} - 1$. Denote by B the matrix A^{2^k}. Then we write

$$U(A) = U_0(A) + BU_1(A) + \ldots + B^{2^k-1} U_{2^k-1}(A).$$

It is then seen that U(A) can then be computed with $3(2^k - 1)$ matrix multiplications of size n and $n^2 t$ elementary products.

For the second algorithm, then U(A)B is first computed for a well chosen invertible matrix B. Passing from U(A)B to U(A) is $O(n^3)$. We take for B the matrix formed by the independent columns

$$\left\{x_1, Ax_1, \ldots, A^{l_1}x_1,\ x_2, Ax_2, \ldots, A^{l_2}x_2,\ \ldots,\ x_m, Ax_m, \ldots, A^{l_m}x_m\right\}$$

where $l_1 + l_2 + \ldots + l_m = n$ and where each l_i is the largest integer for which the set of columns of B formed by $A^{l_i}x_i$ and the previous ones is independent. The vectors $x_1, x_2, \ldots, x_m$ are taken at random under those conditions. The function c(n) is the expected number of factors of a characteristic polynomial. Clearly the expected number for m is bounded from above by c(n). The cost of constructing B is $O(n^3)$ as we have to be able to select the successive x_i's not in the span of the previous vectors.

G. E. COLLINS.

Some Aspects of Univariate Integral Polynomial Factorization.

Topics considered include the utilization of special programs for every small primes and the use of arrays for distinct-degree factorization and Berlekamp's algorithm, optimal use of Musser's factor degree sets, several enhancements of Wang's early factor detection method, a Lehmer-type version of the modular residue to rational number conversion algorithm, and utilization of the partial factor coefficient bound of Beauzamy, Trevisan and Wang.

G. FREY.

On the Discrete Logarithm in Jacobians of Curves.

We are discussing realizations of the cyclic group C_m (m a prime power) inside the group of rational points of $Pic^0(C)$ where C is a curve with arithmetical genus g defined over a finite field $\mathbb{F}_q$ with q elements. To make this realization interesting for public key cryptosystems two conditions have to be satisfied:

1.) Given two rational positive divisors A_1, A_2 of degree g of C one has to be able to find a divisor A_3 with the same properties and a function h of C with $A_1 + A_2 - A_3 = (h) + gP_0$ where $P_0 \in C(\mathbb{F}_q)$ is fixed. If this can be done, we have a fast exponation in $Pic^0(C)$.

2.) There must not exist a fast inverse function "log" of the exponation.

It is easy to see that condition 1 is satisfied for curves C of genus 1 (hence $Pic^0(C) = G_a$, G_m or an elliptic curve); by work of Cantor and more recently by Kampkötter and Spallek one sees that hyperelliptic curves (and especially curves of genus 2) can be handled, too. It is obvious that G_a does not satisfy condition 2, and the use of G_m (which leads to the classical discrete logarithm in $\mathbb{F}_q^*$) is at least dubious because of work of Odlyzko.

So the most interesting curves are elliptic curves and curves of genus 2. The construction of such curves with suitable group of rational points in Pic^0 can be done by random choice and counting points by a Schoof-type algorithm (till now only tolerably fast for elliptic curves) or by using the theory of CM-varieties over number fields (implemented for elliptic curves and in preparation for curves of genus 2), and it is very easy to find a lot of good candidates by these procedures.

Concerning condition 2: In a joint paper with H.-G. RÜCK we show that for any curve C and any natural number m there is a non degenerate pairing from

$$\mathrm{Pic}^0(C)(\mathbb{F}_q(\zeta_m)) \times H^1(G_{\mathbb{F}_q(\zeta_m)}, \mathrm{Pic}^0(\mathbb{F}_q)) \quad \text{to} \quad \mathbb{F}_q^*(\zeta_m)/\mathbb{F}_q(\zeta_m)^{*m}$$

which can be computed in $O(\log m)$ steps of the type described in 1.). So if $\zeta_m \in \mathbb{F}_q$, the log in $\mathrm{Pic}^0(C)$ is reduced to the logarithm in $\mathbb{F}_q^*$, and C should be avoided. This applies for instance to supersingular curves.

Behind the pairing mentioned above is the Tate pairing for Abelian varieties of p-adic fields K'_p which has values in the Brauer group of K_p, and so it seems to be necessary to study those Brauer groups both over K_p (and because of the sum formula for invariants) over number fields more closely.

J. VON ZUR GATHEN.
Factoring Polynomials over Finite Fields.

The factorization of polynomials is a fundamental problem in Computer Algebra. This talk considers polynomials in one variable over a finite field. The important (probabilistic) algorithm of Cantor and Zassenhaus (1981) can (probably) factor a polynomial of degree n in $\mathbb{F}_q[x]$ with an essentially cubic number $O(n^2 \log q)$ of operations in $\mathbb{F}_q$. I present an algorithm that uses an essentially (i.e., disregarding factors of $\log n$) quadratic number of $O(n^2 + n \log q)$ of operations.

This is joined work with V. SHOUP.

W. GEISELMANN.
Selfdual Bases in $\mathbb{F}_{q^n}$.

In this talk weakly selfdual bases and selfdual bases of the field extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are characterized. An equivalence of the symmetry of the $n \times n$-matrices (the matrix representations of the multiplication with elements in $\mathbb{F}_{q^n}$ with respect to the basis used) and the (weakly) selfduality of the basis is shown.

This concept of duality is used to analyze normal basis multiplication in finite fields.

W. GLEISSNER.

Chaos in p-adic Fields.

The convergence of a sequence $\{x_i\}_{i \in \mathbb{N}_0}$ defined by the " chaotic equation " $x_{i+1} = x_i^2 + c$ is investigated using the p-adic norm. It is assumed that $x_0, c \in \mathbb{Q}_p$. One has to distinguish the following cases.

(1) $p^{\hat{k}} \mid (x_0, c)$, $\hat{k}$ maximal
$\Rightarrow |x_i|_p = p^{-k_0} \quad \forall\, i > i_0$, where $p^{k_0} \mid c$, k_0 maximal.

(2) $(x_0, c) = 1$ and $p^{k_0} \mid c$, k_0 maximal
$\Rightarrow |x_i|_p = 1 \quad \forall\, i \in \mathbb{N}_0$.

(3) $(x_0, c) = 1$ and $p \nmid c$.

The sequence $\{x_i \bmod p\}_{i \in \mathbb{N}_0}$ is eventually cyclic. Let l denote the length of the cycle. Choose i_0 such that $x_{i+l} \equiv x_i \bmod p$ for all $i \geq i_0$. If the cyclic part of $\{x_i \bmod p\}_{i \in \mathbb{N}_0}$ does not contain zero then $|x_i|_p = 1 \ \forall\, i \geq i_0$. If zero is in the cyclic part of $\{x_i \bmod p\}_{i \in \mathbb{N}_0}$ then i_0 is chosen such that $x_{i_0} = 0$. Let k be maximal with respect to $p^k \mid x_{i_0}$. The sequence $\{x_i\}_{i \in \mathbb{N}_0}$ has l distinct cluster points, namely

$$y_0 = \lim_{i \to \infty} (x_{i_0 + il}) \qquad \text{with} \quad |y_0|_p = p^{-k}$$

$$y_j = \lim_{i \to \infty} (x_{i_0 + j + il}) \qquad \text{with} \quad |y_j|_p = 1, \quad 1 \leq j < l.$$

Furthermore, one can derive that for all prime numbers p, q, $(p,q) = 1$, and for all $m \in \mathbb{N}$ $\exists\, n \in \mathbb{N}$ such that $p^m \mid (q^n - 1)$.

J. GRABMEIER.

Genetics in AXIOM.

Non-associative algebras appear in applications e.g. as Lie algebras of symmetries of partial differential equations. Another interesting class of such algebras appear if one wants to model Gregor Mendel's laws of genetic inheritance:

$$Aa \times Aa = \frac{1}{4} AA + \frac{1}{2} Aa + \frac{1}{4} aa.$$

In gametic algebras the different gametes $a_1 \dots a_n$ of a population constitute a basis (over $\mathbb{R}$ or $\mathbb{C}$). The segregation rates in sufficiently large random mating populations for the zygots (= products of basis elements) are just the structural constants:

$$a_i a_j = \sum_k \gamma_{ij}^{(k)} a_k \qquad (0 \le \gamma_{ij}^{(k)} \le 1, \ \sum_k \gamma_{ij}^{(k)} = 1).$$

Vectors of weight 1 describe populations, the product $x*y$ describes the filial generation of mating populations x and y. If there are no sexual dependencies these are commutative and non-associative algebras. Typical problems to be studied are: idempotents (equilibrial states), convergence of powers of various kinds of weight 1-vectors and classification of such algebras for small ranks.

In a joint work with R. WISBAUER we have implemented a non-associative "world" in the computer algebra system AXIOM providing categories like Monad, NonAssociativeAlgebra and domains as AlgebraGivenByStructuralConstants and GenericNonAssociativeAlgebras and functions which allow to solve typical problems (Is an identity like Jacobi's valid? Construct a basis of the middle nucleus).

This setting allows to easily define arbitrary algebras of finite rank and compute with them in AXIOM, and - of course - can be used to study also the genetic algebras.

A. GUTHMANN.
Primality Testing Algorithms for Integer Approximation to l-adic Roots of Unity.

Effective tests for primality are given for integers N satisfying $|N-\eta|_l \le l^{-n}$ ($l > 2$ a prime, η an $(l-1)$st root of unity in $\mathbb{Z}_l$).

D. HACHENBERGER.
On the Existence of Completely Free Elements in a Finite Field.

Let $q > 1$ be a prime power, $m > 1$ an integer and $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$ the Galois fields of order q^m and q, respectively. In 1986, Journal of Algebra 103, 141-159, D. Blessenohl and K. Johnsen have proved that there exists an element w in $\mathbb{F}_{q^m}$ such that w generates a normal basis over <u>any</u> intermediate field $\mathbb{F}_{q^r}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Such elements are called completely free in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

The existence of such an element is easily reduced to the special case where m is a prime power. In order to settle the problem in this special case, Blessenohl and Johnsen mainly use representation theory of finite abelian groups. Although their proof could slightly be condensed in a supplement by D. Blessenohl in Journal of Algebra 132, (1990), 154 - 159, it is still involved.

The aim of my talk is to present a detailed and constructive proof of the theorem of Blessenohl and Johnsen by using essentially some basic properties of cyclotomic polynomials over finite fields. Furthermore, we give a recursive formula for the number of completely free elements in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ in the case where m is a prime power.

H. HONG.
Topology Analysis of Plane Real Algebraic Curves.

We give an efficient algorithm which, given a bivariate polynomial, constructs a planar graph topologically equivalent to the plane curve defined by the polynomial.

The algorithm follows the general structure:

1) finding all "interesting" points,
2) counting the numbers of left/right branches,
3) connecting up the points according to the branch counts.

The efficiency of the algorithm is due to elimination of expensive operations with real algebraic numbers such as gcd, division, and root bound computation. This is achieved by the theory of subresultants and Sturm sequence.

The current implementation can handle dense polynomials of total degree 16 within 1 minute.

T. JEBELEAN.
Systolic Multiprecision Arithmetic.

This is an overview of a research aimed at speeding-up Computer Algebra systems by systolic parallelization of the arithmetic of long integers and long rationals. This is important because long integer arithmetic tends to consume most of the computation time in large applications (e.g. Gröbner bases).

A new algorithm for *exact division* (i.e. division with null remainder) was designed which is also suitable for systolic implementation in the *least-significant digits first (LSF)* pipelined manner. After binary-shifting the operands until they become odd, q_0 (the LS digit of the quotient) can be found from c_0 and a_0 (the LS digits of the dividend and divisor) by:

$$b_0 = (c_0 * a_0^{-1}) \bmod \beta.$$

The process is iterated after subtracting from the dividend b_0 multiplied with the divisor.

A *generalization of the binary GCD algorithm* was found, which is also suitable for systolic parallelization in LSF pipelined manner, and is also faster than the currently used GCD algorithms even in the sequential implementation. After binary-shifting the operands until they become odd, one takes a, b (the least-significant *double-words* of the operands), and one finds two "modular conjugates" x, y which are at most *one word* long, with the property

$$(x*a \pm y*b) \bmod \beta^2 = 0.$$

By this process, one operand is reduced by one word, and then the other operand can be reduced by one word by using the "exact division" scheme. Hence, all the important algorithms required by multiprecision rational arithmetic can be aggregated in systolic LSF pipelined manner.

J. JOHNSON.
The Coefficient Sign Variation Method for Real Root Isolation.

An algorithm for isolating the real roots of a polynomial is discussed. The algorithm is based on Descarte's rule of signs and a sequence of polynomial transformations. The transformations correspond to the continued fraction expansions of the roots. This algorithm was originally presented by Vincent (1836), and modified by Akritas (1978). However, both of those algorithms have exponential computing time. We modify Vincent's algorithm to obtain a polynomial computing time bound, and compare it to a similar algorithm with polynomial computing time due to Collins and Akritas. The behaviour of the algorithm is related to the distribution of partial quotients.

D. JUNGNICKEL.

Almost Perfect Binary Sequences.

Let $\alpha := (a_n)_{n \in \mathbb{N}}$ be a binary sequence with period v. The autocorrelation coefficients c_t are defined as the number of agreements minus the number of disagreements of α with the t-fold shifted sequence $(a_{n+t})_{n \in \mathbb{N}}$. For applications in signal processing, one would like to have perfect binary sequences, i.e., $c_t = 0$ whenever t is not a multiple of v. Unfortunately, only the case $v = 4$ is known; in fact one generally conjectures non-existence for all larger v. This is equivalent to the non-existence of cyclic Hadamard matrices and known to be true for $v < 12100$. Recently, J. Wolfmann studied almost perfect binary sequences where one allows to have $c_t \neq 0$ for one non-trivial congruence class modulo v. With the help of some theoretical observations, Wolfmann constructed such sequences with exactly $2m-1$ entries +1 per period for all $v = 4m$ (v has to be divisible by 4) with $v \leq 100$, $v \neq 32, 44, 68, 72, 80, 92$. The purpose of this talk is to report on the following nice observation by my former doctoral student A. POTT:

Theorem. An almost perfect binary sequence with f entries +1 per period exists if and only if there exists a cyclic divisible difference set with parameters

$$\left(\frac{v}{2}, 2, f, (f-\frac{v}{2})(f-\frac{v}{2}+1), f-\frac{v}{4}\right).$$

Corollary. The case $f = 1$ corresponds to cyclic relative difference sets with parameters

$$\left(\frac{v}{2}, 2, \frac{v}{2}-1, \frac{v}{4}-1\right).$$

By a classical construction of Bose, the affine geometry AG(2, q) can be represented by a cyclic relative difference set with parameters $(q+1, q-1, q, 1)$. A projection argument gives the desired examples for $\frac{v}{2} - 1$ an odd prime power. Delsarte, Goethals and Seidel (1971) conjectured that these are the only possible parameters and verified this for $v \leq 452$ (using algebraic techniques). Hence:

Corollary. Almost perfect binary sequences with period $v \leq 452$ and $\frac{v}{2} - 1$ entries +1 per period exist if and only if $\frac{v}{2} - 1$ is an odd prime power.

Hence Pott answered the questions posed by Wolfmann.

E. KALTOFEN.
Parallel Solution of Sparse Linear Systems with Symbolic Entries.

We discuss a variant of Wiedemann's "coordinate recurrence" method, due to Coppersmith, that allows the solution of a linear system on n processors in $O(N^2 \log N)$ parallel time, N the dimensions of the coefficient matrix, and $2N/n + O(1)$ parallel multiplications of that matrix by vectors. The algorithm uses randomization and computes the solution exactly. All these precise complexity measures follow from our probabilistic analysis of Coppersmith's method.

We also report on experimental results when executing this algorithm on a network of computers. E.g., we can solve a 20000 by 20000 system with ≈ 1300000 non-zero entries from the finite field $GF(2^{15} - 19)$ on 8 SUN-4 computers (rated 28.5 MIPS) in about 57 hours. We propose the challenge of solving a 100000 by 100000 system with 10 million non-zero entries from the field $GF(2^{32} - 5)$ on a network of computers in a reasonable amount of time, say one week.

A. KERBER.
Algebraic Combinatorics via Finite Group Actions.

This talk was a report on joint work with R. LAUE, R. GRUND and B. SCHMALZ on the constructive theory of discrete structures (e.g. graphs, molecular graphs, t-designs). Emphasize was laid on basic methods which are particular cases of the Homomorphism Principle: Blocks and orbit transversals as well as double coset methods. As an application of this to t-designs it was pointed to the results of B. Schmalz, who obtained complete lists of designs with prescribed automorphism group as well as to our program system MOLGEN that allows to generate the molecular graphs that correspond to a given brutto formula.

M. KLIN.

Schur Rings over Cyclic Groups and Automorphism Groups of Circulant Graphs.

Let $\Gamma = \Gamma(\mathbb{Z}_n, X)$ be an n-vertex circulant graph with a connecting set $X \subseteq \mathbb{Z}_n$. This means that Γ has vertex set $\mathbb{Z}_n$ and a set $\{ (a, a+x) \mid a \in \mathbb{Z}_n, x \in X \}$ of arcs. Γ can be treated as undirected graph if $-X = X$. We consider the problem of description of automorphism groups of circulant graphs. Here the case $n = p^3$, p a prime is considered. We use results on enumeration of S-rings (Schur rings) over cyclic groups. The description is recursive and uses information about the cases $n = p$, p^2 (Klin/Pöschel).

All uniprimitive permuation groups of degree p (Frobenius groups) and the symmetric group S_p are called p-atoms. The symmetric group $S_p 2$ and the Frobenius overgroups of $(\mathbb{Z}_{p^2}, \mathbb{Z}_{p^2})$ form the set of p^2-atoms.

Theorem. Every automorphism group of a p^3-vertex circulant graph (p an odd prime) belongs to one of the following types:

a) a wreath product of a p-atom and a p^2-atom or vice versa;

b) a wreath product of three p-atoms;

c) $S_p 3$;

d) a Frobenius group of degree p^3;

e) a 2-closure (in the sense of H. Wielandt) of the permutation group $(G, \mathbb{Z}_p 3)$, where $G = \mathbb{Z}_p 3 \lambda H$, $H < \mathbb{Z}_p 3$, $(1+p^2) \in H$, $(1+p) \not\in H$.

There are altogether $1 + 4u_p + 2u_p^2 + u_p^3$ different groups (here u_p is a number of divisors of $p-1$). The structure of 2-closures in the case e) is also obtained. The case $n = 8$ requires special consideration, there are 10 automorphism groups in this case.

W. KRANDICK.

High Precision Calculation of Real and Complex Polynomial Roots.

A straightforward implementation of Newton's method for polynomial real root calculation using exact arithmetic on rational numbers is unacceptably slow, because in each step the length of the iterate multiplies by the degree of the polynomial. We present an infallible algorithm which keeps the length of each approximation proportional to its accuracy. The resulting speed-up is dramatic. A further speed-up is obtained by using a heuristic scheme involving floating point arithmetic and interval arithmetic; the exact algorithm then serves as a backup.

Next we show how real root calculation can be used for complex root calculation. A rectangle which contains exactly one complex root of a univariate polynomial has to be refined in highly convergent steps.

The complex root is the unique point inside the rectangle where a certain pair of plane algebraic curves intersect. Each curve will usually intersect the rectangle in exactly two points. These points can be found by real root calculation. The tangents to the curve in those points will in most instances form a triangle with the secant connecting the points, and the triangle will contain the part of the curve which lies inside the rectangle. The intersection of the two triangles for the respective curves will then contain the complex root. A new rectangle is constructed which contains this intersection. After each such refinement step an infallible winding number computation decides whether this rectangle does indeed contain the root. These verification steps spend almost all of their time computing the points where the curves intersect the new rectangle, i.e. they effectively prepare the next refinement step. Hence, only the time for the last winding number computation is extra time. If the tangent-secant heuristic fails, bisection is used for refinement.

K. Lehr.
Natürliche Konstruktionen.

Nach einigen historischen Bemerkungen über einerseits Kollraidev, Robleiano, Saito et al., Maltsiniotis und andererseits Foata, Garsia-Milne, Stanley, Paule, Feldman-Propp gebe ich einen Vergleich der alten Kürzungsmethode von Tarski, die eine Prioritätsordnung und einen vollstrukturierten Faktor erfordert, mit der neuen von Feldman-Propp, die auf endliche Objekte zugeschnitten ist, dafür aber nurmehr die Punktierung des zu kürzenden Faktors braucht.

Mit den klassischen Ideen im Rücken und Feldman-Propps neuer Methode kürze ich Potenzen mit vollstrukturiertem Exponenten, eine Aufgabe, die Feldman-Propp mit Bedauern nicht bewältigten. Daneben betrachte ich Analoga in anderen Kategorien (z.B. Vektorräumen). Dabei stellt sich Banascharskis CSB-Banach-Satz als im "natürlichen" Sinne falsch heraus. Algorithmisch interessant erscheint die Frage nach der Anzahl der in den Konstruktionen erforderlichen "Zellen".

T. MORA.

Gröbner Basis and the Word Problem.

If computable, Gröbner bases in a non-commutative free algebra allow to solve the real membership problem and so the undecidable word problem.

It can be seen that the only obstruction to computability of Gröbner bases is that they can be infinite. In fact, there is a procedure which halts if and only if the Gröbner basis is finite, in which case it returns it.

A same ideal has different Gröbner bases, according to an ordering imposed on the free semigroup. If a dense set of orderings exists (i.e. a set $\mathcal{P}$ of orderings such that if an ordering exists satisfying finitely many given disepurtion then there is such an ordering in $\mathcal{P}$), then if an ideal has just a single finite Gröbner basis, its membership problem is solvable.

There are, however, instances of a solvable word problem, whose corresponding ideal has no finite Gröbner basis at all.

O. MORENO.

Improvements on the Ax- Katz Theorem, a p-adic Serre's Bound and Weights of Duals of BCH Codes.

Research Problem 9.5 of MacWilliams and Sloane's book *The Theory of Error Correcting Codes* asks for an improvement of the minimum distance bound of the duals of BCH codes, defined over $\mathbb{F}_{2^m}$, m odd. The objective of the present talk is to give a solution to the above problem by:

(i) obtaining an improvement to the Ax theorem, that we prove is best possible for many classes of examples,

(ii) establishing a sharp estimate for the relevant exponential sums which implies a very good improvement for the minimum distance bound,

(iii) providing a doubly infinite family of counter examples to Problem 9.5 where both the designed distance and the length increase independently,

(iv) verifying that our bound is tight for some of the counterexamples, and

(v) in the case of even m we give a doubly infinite family of examples where the Carlitz-Uchiyama bound is tight, and in this way determine the exact minimum distance of the duals of the corresponding BCH codes.

J. MÜLLER-QUADE.
Parallel Decomposition of Ω-Algebras.

Motivated from divide and conquer and product automata I introduce a very general parallel decomposition of Ω-Algebras. It even allows the parts to grow bigger than the original. In spite of the many new chances some Ω-Algebras, like natural numbers or finite simple groups, remain undecomposable.

I conclude with an outlook to parallel products that allow the parts to communicate.

U. OBERST.
The Solvability and the Constructive Solution of Linear Systems of Partial Difference Equations with Constant Coefficients - A Survey.

In the talk I discussed the problems of the title. The lecture was based on the work of the *Multidimensional System Group*, Innsbruck, consisting of the speaker and the graduate students S. KLEON, S. RITKEAO, S. WALCH and E. ZERZ, and in particular on the following papers:

(1) U.O.: Multidimensional Constant Linear Systems, Acta Appl. Math. 20 (1990), 1-175.

(2) U.O.: Finite Dimensional Systems of Partial Differential or Difference Equations, submitted to Adv. of Math., June 1992.

(3) U.O.: Variations on the Fundamental Principle for Linear Systems of Partial Differential or Difference Equations with Constant Coefficients, subm. to AAECC, January 1993.

(4) E. Zerz, U.O.: The Canonical Cauchy Problem for Linear Systems of Partial Difference Equations with Constant Coefficients over the Complete Integral Lattice $\mathbb{Z}^r$.

A written report on the results was handed out to several interested colleagues.

The problems are both canonically formulated and algorithmically solved by means of Gröbner basis methods. The solution of the Cauchy or initial value problem is significant for various applied fields, in particular for digital image processing, and also for the numerical solution of hyperbolic systems of partial differential equations by the method of finite differences. A look into recent books on difference equations, for instance Kelley-Peterson, Difference Equations, Academic Press 1991, shows that even for a single equation in two dimensions the hitherto existing results in this area were very rudimentary contrary to the huge body of results on partial *differential* equations.

J. OKNINSKI.
Linear Semigroups. Results and Applications.

A structure theorem for an arbitrary subsemigroup S of the full linear monoid $M_n(K)$ over a field K is given. It associates to S a collection of at most 2^n linear groups G_α and as many "sandwich matrices" P_α over these groups. The strategy is then to study S via the group actions of the G_α's on themselves and on the matrices P_α. As an application we discuss the growth problem for S.

The class of (finite) monoids of Lie type, built on a group G of Lie type, is presented. The basic example being $M = M_n(\mathbb{F}_q)$ with $G = GL_n(\mathbb{F}_q)$. Such monoids can be locally "covered" by a universal monoid $\mathbb{M}$ on G, that admits a very nice linear representation theory. Moreover, combinatorics on $\mathbb{M}$ can often be reduced to combinatorics on G. This leads to several consequences that had not been known even for $M = M_n(\mathbb{F}_q)$.

V. PAN.
Supereffective Slow-Down of Algebraic Computations.

It is customary to measure the complexity of parallel computations by time and number of processors used. To resolve the problem of the trade-off between these two measures, we adapt the policy suggested by practice of computations: we devise the algorithms whose potential work (that is, the product of time and processor bounds) stays at the level of the best available sequential time bound, and we minimize the parallel time under this assumption.

We reach these goals or achieve a substantial progress in this direction for several fundamental problems of matrix and polynomial computations, including solving linear systems and matrix inversion over fields and semirings (with further applications to computation of paths in graphs), in the cases of general, triangular and structured matrices, as well as polynomial division and computation of the square or the m-th root of a polynomial modulo a power. This is achieved by combining the techniques of stream contraction, recursive restarting of computations and effective slow-down of parallel computations, which we make supereffective, that is, we decrease the processor bound by the factor of s by means of the slow-down by o(s) times. Part of the work was done in cooperation with F.P. PREPARATA (on matrix computations) and with D. BINI (on polynomial computation).

D. POLEMI.
Singular Algebraic Curves.

We analyze and compare different methods to resolve the singularities of an algebraic curve (classical method, accessible geometric method, algebraic method).

Based on the Brill-Noether theorem we describe two polynomial algorithms for effectively constructing the Riemann-Roch theorem, finding the genus, adding points on the Jacobian of a singular curve, constructing algebraic geometric Goppa codes from singular curves.

A. POLI.
Another Manner to Enumerate SCN Bases.

In the Proceedings of the AAECC 4 Conference (Karlsruhe, 1986) we develop a method to construct and enumerate Self Dual Multicirculant Codes over $\mathbb{F}_2$ and $\mathbb{F}_3$. We used n-variable polynomials. In "Error Correcting Codes: Theory and Applications" (by A. Poli and Ll. Huguet, Masson 1989 and Prentice Hall 1992) we generalize these results.

Here, we apply our formulas to the elementary case (one variable) which corresponds to self normal bases. That the enumeration of SCN bases can be expressed in terms of one variable polynomials comes from a result of Wang (1989).

The enumeration of these SCN bases is already published in 1990, by Jungnickel et al., but in a different way.

F. SCHAEFER - LORINSER.
Construction of Elliptic Curve Cryptosystems.

Elliptic curves over finite fields are proposed for the construction of one-way functions. To avoid the efficient applicability of the fastest known discrete logarithm algorithms, one is interested in the construction of elliptic curve groups with certain properties.

Several algorithms to count the number of points on elliptic curves based on the algorithm of Schoof are considered. An alternative approach using the Weyl-conjecture to find examples of curves with coefficients from small subfields is proposed.

Final remarks consider the possibilities to implement the arithmetic on elliptic curves over finite fields of characteristic 2 in hardware.

W. SCHARLAU.
Construction of Good Binary Codes.

We report on various methods to construct binary linear codes of moderate length ($n \leq 127$, or $n \leq 255$) explicitely. These methods include improvements of well known constructions in coding theory, e.g. punchering, shortening, X-construction, transfer, Blokh-Zybalov construction. Extensive use of computers leads to many improvements in the tables of the best known codes. The results are due to my students WIRTZ, SCHOMAKER, BERNTZEN, GRONEICK, GROSSE, KEMPER.

W. SCHEMPP.

The Heisenberg Lie Algebra and Neural Network Computations.

The purpose of this lecture is to indicate the role of the Heisenberg nilpotent Lie algebra in computational tomography, computational holography, and neural network computations. In particular its role for fast algorithms implementing adaptive filter models of neural network engineering are described. A video tape will display the underlying hyperbolic geometry.

A. SCHÖNHAGE.

Sharp Bounds for the Perturbation of Polynomial Zeros.

Given monic complex polynomials $f(z) = \prod_{i=1}^{n} (z-u_i)$, $g(z) = \prod_{j=1}^{n} (z-v_j)$ with $|u_i|, |v_j| \le 1$ and l_1-norm deviation $|f-g|_1 = \varepsilon$, the problem is to find a sharp bound for $\delta(f,g) = \min_\pi \max_i |u_i - v_{\pi(i)}|$. $f = z^n$, $g = z^n - \varepsilon$ amounts to $\delta = \sqrt[n]{\varepsilon}$. Ostrowski's bound $\delta \le (2n-1)\sqrt[n]{\varepsilon}$ was improved by my 1982 result $\delta \le (4+o(1))\sqrt[n]{\varepsilon}$. Here I present work of my student R. SCHÄTZLE (1990).

Theorem. $\delta(f,g) \le \eta(1+\frac{1}{2}\eta+\frac{1}{8}\eta^2)$, where $\eta = \sqrt[n]{\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor} |f-g|}$;

for $\varepsilon \le 2^{-4n}$, the extra factor $(1+O(\eta))$ is less than 1.065.

Sharpness of this estimate is obtained by examples like a, b with $|a|, |b| < 1$, $|a-b| = \delta$, then define $\varphi(t) = n(t-a)^{k-1}(t-b)^{m-1}$, where $k+m = n+1$, and set $f(z) = \int_a^z \varphi(t)\,dt$, $g(z) = \int_b^z \varphi(t)\,dt$. Then f has k zeros in a, g has m zeros in b, thus $\delta(f,g) \ge \delta$, and $\varepsilon = g-f = \int_a^b \varphi(t)\,dt = \pm\delta^n / \binom{n-1}{k-1}$.

S. A. VANSTONE.

Group Factorizations and their Cryptographic Significance.

Let G be finite group and $F = \{A_j \subseteq G \mid 1 \le j \le t,\ t \ge 2,\ |A_i| \ge 2\}$. F is called a factorization of G if

(i) $G = A_1 A_2 \dots A_t$ and

(ii) $|G| = \prod_{j=1}^{t} |A_j|$.

Group factorizations were introduced in the early 1940's as a tool to solve a famous conjecture of Minkowski and then reintroduced in the mid 1980's as an algebraic structure on which to base a private key cryptographic scheme. Our interest is to try to construct a public key system on these structures. In this lecture we give a brief survey of knapsack "like" schemes and then discuss some recent work with M. Qu on group factorizations and how they can be applied to public key cryptography.

K.-H. Zimmermann.
On the Decoding of Modular Group Codes.

Given. K (finite field of characteristic p) and G (finite p-group). Then the augmentation ideal

$$I_K(G) = \{ \sum_{g \in G} k_g g \in KG \mid \sum_{g \in G} k_g = 0 \}$$

of KG equals the Jacobson radical of KG.

Given. A filtration of $I_K(G)$:

$$I_K(G) = I_1 \supseteq I_2 \supseteq \ldots \supseteq I_T \supseteq \ldots$$

i.e., I_j is an ideal of KG and $I_j I_k \subseteq I_{j+k}$ for all $j, k \geq 1$.

By considering I_j as a linear code in the ambient space KG, we obtain the following

Result. If $p = 2$ then each code I_t is completely majority decodable.
(This was known before only for binary Reed - Muller codes.)

In case of $p > 2$ we can provide a lower bound on the number of errors which can be corrected by majority decoding.

Berichterstatter: D. Hachenberger.

Tagungsteilnehmer

Dr. Robert Beals
Department of Mathematics and
Computer Science, University of
Chicago, Ryerson Hall
1100 East 58th St.

Chicago , IL 60637
USA

Prof.Dr. George E. Collins
Research Institute for Symbolic
Computation
Schloß Hagenberg

A-4232 Hagenberg

Prof.Dr. Thomas Beth
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5, Geb. 5034

W-7500 Karlsruhe 1
GERMANY

Prof.Dr. Gerhard Frey
Institut für Experimentelle
Mathematik
Universität-Gesamthochschule Essen
Ellernstr. 29

W-4300 Essen 12
GERMANY

Prof.Dr. Bruno Buchberger
RISC (Research Institute for
Symbolic Computation)
Universität Linz

A-4040 Linz

Prof.Dr. Joachim von zur Gathen
Department of Computer Science
University of Toronto
10 Kings College Road

Toronto, Ontario , M5S 1A4
CANADA

Prof.Dr. Jacques Calmet
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5, Geb. 5034

W-7500 Karlsruhe 1
GERMANY

Willi Geiselmann
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5, Geb. 5034

W-7500 Karlsruhe 1
GERMANY

Prof.Dr. Paul Camion
INRIA Rocquencourt
Domaine de Voluceau
B. P. 105

F-78153 Le Chesnay Cedex

Dr. Winfried Gleissner
Schleißheimer Str. 209

W-8000 München 40
GERMANY

Dr. Johannes Grabmeier
IBM Deutschland Informations-
systeme GmbH
Wissenschaftliches Zentrum
Vangerowstr. 18. PF 103068

W-6900 Heidelberg
GERMANY

Dr. Andreas Guthmann
Fachbereich Mathematik
Universität Kaiserslautern
Postfach 3049

W-6750 Kaiserslautern
GERMANY

Dr. Dirk Hachenberger
Fachbereich Mathematik
Universität Kaiserslautern
Postfach 3049

W-6750 Kaiserslautern
GERMANY

Dr. Hoon Hong
RISC (Research Institute for
Symbolic Computation)
Universität Linz

A-4040 Linz

Tudor Jebelean
Research Institut for Symbolic
Computation
Schloß Hagenberg

A-4232 Hagenberg

Prof.Dr. Jeremy R. Johnson
Department of Mathematics
and Computer Science
Drexel University

Philadelphia , PA 19104
USA

Prof.Dr. Dieter Jungnickel
Institut für Mathematik
Universität Augsburg
Universitätsstr. 8

W-8900 Augsburg
GERMANY

Prof.Dr. Erich Kaltofen
Department of Computer Science
Rensselaer Polytechnic Institute

Troy , NY 12180-3590
USA

Prof.Dr. Adalbert Kerber
Fakultät für Mathematik und Physik
Universität Bayreuth
Postfach 10 12 51

W-8580 Bayreuth
GERMANY

Prof. Dr. Mikhail H. Klin
Department of Mathematics and
Computer Science
Ben-Gurion University of the Negev
P.O.B. 653

84105 Beer-Sheva
ISRAEL

Dr. Werner Krandick
RISC (Research Institute for
Symbolic Computation)
Universität Linz

A-4040 Linz

Dr. Helmut Meyn
Institut für Mathematische
Maschinen und Datenverarbeitung I
Universität Erlangen
Martensstr. 3

W-8520 Erlangen
GERMANY

Prof.Dr. Klaus Leeb
Institut für Informatik I
Universität Erlangen
Martensstr. 3

W-8520 Erlangen
GERMANY

Prof.Dr. Teo Mora
Istituto di Matematica
Universita di Genova
Via L. B. Alberti, 4

I-16132 Genova

Prof.Dr. Rüdiger Loos
Fakultät für Informatik
Universität Tübingen
Sand 13

W-7400 Tübingen
GERMANY

Prof.Dr. Oscar Moreno
Dept. of Mathematics
Faculty of Natural Sciences
University of Puerto Rico
Box 23355

Rio Piedras , PR 00931
USA

Prof.Dr. Heinz Lüneburg
Fachbereich Mathematik
Universität Kaiserslautern
Postfach 3049

W-6750 Kaiserslautern
GERMANY

Jörn Müller-Quade
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5, Geb. 5034

W-7500 Karlsruhe 1
GERMANY

Martin Lüneburg
Fakultät für Mathematik
Universität Bielefeld
Postfach 10 01 31

W-4800 Bielefeld 1
GERMANY

Prof.Dr. Ulrich Oberst
Institut für Mathematik
Universität Innsbruck
Technikerstr. 15

A-6020 Innsbruck

Prof.Dr. Jan Okninski
Mathematisches Institut
Universität Freiburg
Albertstr. 23b

W-7800 Freiburg
GERMANY

Prof.Dr. Winfried Scharlau
Mathematisches Institut
Universität Münster
Einsteinstr. 62

W-4400 Münster
GERMANY

Prof.Dr. Victor Y. Pan
Lehman College
The City University of New York
Bedford Park Boulevd., West

Bronx , NY 10468-1589
USA

Prof.Dr. Walter Schempp
Lehrstuhl für Mathematik I
Universität Siegen
Postfach 10 12 40
Hölderlinstr. 3

W-5900 Siegen
GERMANY

Prof.Dr. Despina Polemis
Mathematics Department
Baruch College
City University of New York
17, Lexington Avenue

New York , N. Y. 10010
USA

Prof.Dr. Arnold Schönhage
Institut für Informatik II
Universität Bonn
Römerstraße 164

W-5300 Bonn 1
GERMANY

Prof.Dr. Alain Poli
Laboratoire AAECC-IRIT
Université Paul Sabatier
118, route de Narbonne

F-31062 Toulouse Cedex

Prof.Dr. Scott A. Vanstone
Department of Combinatorics and
Optimization
University of Waterloo

Waterloo , Ont. N2L 3G1
CANADA

Frank Schaefer-Lorinser
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5, Geb. 5034

W-7500 Karlsruhe 1
GERMANY

Dr. Karl-Heinz Zimmermann
Mathematisches Institut
Universität Bayreuth
Postfach 10 12 51

W-8580 Bayreuth
GERMANY