MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 1/1989

Applicable Algebra

1.1. bis 6.1.1989

The first meeting of the year 1989, dedicated to the area of Applicable Algebra, was the second on this topic held at Oberwolfach after the first conference on "Anwendbare Algebra" in early 1983.

For this year's conference the program had been planned by the three organizers Thomas Beth (Karlsruhe), Bruno Buchberger (Linz) and Heinz Lüneburg (Kaiserslautern) to address areas from Algebra and its applications, like computer aided design, image processing, communications engineering, digital signal processing, inverse kinematics, inverse dynamics, robot programming, geometrical modelling, abstract data types, artificial intelligence, VLSI-Design and verification.

The meeting, which started on the afternoon of New Year's Day brought together 36 people of 9 countries. As planned by the organizers, the emphasis was on such applications which require solution methodologies from typical algebraic areas such as: Arithmetics in real, complex and finite fields, discrete mathematics, representation theory, algebraic theories, algebraic logic and algebraic geometry.

The talk by Schröder (Göttingen) surveyed the manyfold applications of number theory, finite field arithmetics and elementary group theory to the areas of communications, engineering and acoustics. The general overview by Rembold (Karlsruhe) gave a wide scope introduction to the state of the art and problems arising in the area of robotics, showing the close relation to problems of computational geometry, algebraic manyfolds, Gröbner bases and artificial intelligence. The surveyes by Kanatani (Gunma) and Nagel (Karlsruhe) on the problems encountered in Vision related to Representation Theory and Artificial Intelligence.

These talks set the frame for the subsequent talks which can be grouped into three major areas, namely Computer Algebra, computational geometry and arithmetics with close interrelations between these three fields. The questions addressed in computational geometry reached from problems of classical manyfold theory to problems of stereogrammetry while touching upon problems of arithmetics in complex

number fields. Simultaneously methods of model theory of theorem proving were employed. The close connections of finite field arithmetics to pseudo-random generation and coding theory again led to questions of VLSI-design problems, an area which is also closely related to computational geometry.

During several problem and discussion sessions held in the evenings it became clear, that a general common topic for most problems addressed should be seen under the classical title "Invariant Theory". After a survey talk by Abhyankar one of the organizers showed in a tour d'horizon many close relations between invariant theory techniques in program design, coding theory, vision and problems of geometry. It was felt that the results of these discussions led to a new insight into the area of applicable algebra in both applied mathematics and computer science.

It has become clear through this conference that an essential topic in the areas considered lead to common approach of problems solving, which could be entitled by the headlines "symmetry finding" as a process of further research work into the area of modern invariant theory. Though it may seem that the results of this discussion inevitably lead to classical group theory it has become obvious that the research topics to be addressed in this context will make considerable use of algebraic geometry and representation theory on one side but with a clear direction into research areas of modern computer science such as automatic theorem proving, programming in logic, applied model theory and the design of next generation computer algebra systems.

The extremely positive atmosphere of Mathematisches Forschungsinstitut Oberwolfach, supported by pleasant weather and the well-known hospitality of all staff as well as the special support and dedication of the director of the institute, Professor Barner has made it possible to conclude this conference with the extremely positive feeling by all participants as to having gained insights into a new research area which was only founded during this conference at Oberwolfach.

Abstracts

M. R. SCHROEDER: The Unreasonable Effectiveness of Number Theory in Physics, Music and Communication

Number Theory is often thought of as rather abstract and far removed from practical applications. Actually, however, the "higher arithmetic" provides highly useful answers to numerous real-world problems, including the design of musical scales, cryptographic systems, and special phase arrays and diffraction gratings with unusually broad scatter (with applications in radar camouflage, laser speckle removal, noise abatement, and concert hall acoustics). One of the prime domains of number theory is the construction of powerful error-correcting codes, such as those used for picture transmission from space vehicles and in compact discs (CD's). Other applications

include schemes for spread-spectrum communication, "error-free" computing, fast computational algorithms, and precision measurements (of interplanetary distances, for example) at extremely low signal-to-noise ratios. In this manner the "fourth prediction" of General Relativity (the slowing of electromagnetic radiation in gravitational fields) has been fully confirmed. The quasiperiodic route to chaos of nonlinear dynamical systems are being analyzed in terms of continued fractions, Fibonacci numbers, the golden mean and Farey trees. Even the recently discovered new state of matter ("quasicrystals") is effectively described in terms of such number-theoretic principles. And last not least, prime numbers, whose distribution combines regularity and randomness, are a rich source of pleasing artistic designs.

Z. D. DAI: Functions Defined by de Bruijn Sequences (Joint work with K. C. Zeng)

In cryptosystems, one of the ideas is to make use of nonlinear feedforward functions f of linear feedback shift-register sequences. The function f, can be expressed in an unique way as a polynomial in indeterminates linear in each of them separately. f should satisfy n certain cryptographic requirements. The following is a list of the simplest among them.

1. The function f with value range $\{0,1\}$ should be balanced, and complete in the sense that it will contain each of the n indeterminates explicitly.
2. It should have a reasonably high total degree.
3. It should be free from certain correlational weaknesses.
4. The family of functions used should be parametrized by a space $V_l(GF(2))$.

Since de Bruijn sequences can be produced in large numbers, it is natural to think of defining the feedforward function f by means of a de Bruijn sequence

$$\beta = (b_0, b_1, \cdots, b_i, \cdots, b_{2^n-1}; \cdots),$$

by putting

$$f(i_0, i_1, \cdots, i_{n-1}) \;=\; b_i, \qquad i = \sum_{j=0}^{n-1} i_j 2^j,\ i_j = 0 \text{ or } 1.$$

It can be proved that the de Bruijn functions satisfy the above requirements pretty well. For example we have the following theorem.

Theorem If $n \geq 2$, then the function f defined by a de Bruijn sequence of degree n is balanced, complete and $deg(f) \geq \lfloor \log_2 n \rfloor$.

The given lower bound given is by no means discouraging, but it is too modest as compared with results computed for a large number of de Bruijn sequences, so, there is a hope to improve it much. New ideas are needed for improving this bound.

L. BUDACH: VLSI-Design and Fractals

VLSI-technology makes it possible to integrate millions of transistor functions on a chip. In order to use these new possibilities for advanced computer architecture one is led to find hardware realizations of important principles in computation theory. These principles have been developed to find very fast (parallel) algorithms. Many of them - take the divide and conquer principle as an example - lead in a very natural way to a recursive design of algorithms. In order to bring these designs on silicon a system RELACS (REcursive LAyout Computing System) has been developed and implemented in Berlin as common word of Humboldt-University and the Academy of Science of GDR by L. Budach, H. Grassmann, E.G. Giessmann, B. Graw, Ch. Meinel, B. Molzan, U. Schaefer and P. Zienicke. A RELACS-program is characterized by the fact, that not only one boolean function f but a sequence f_n of boolean functions is realized by a uniform design of a sequence V_n of VLSI-layouts. It is proved that in a certain sense V_n converges to a structure V which reflects the mayor qualities of V_n for $n \gg 0$. V can be obtained by a generalization of a method of J.E. Hutchinson [1] for the construction of self-similar fractals. Hutchinsons theorem results as the degeneration of a graph (the generation graph of the RELACS-program) to a single point.

[1] J.E. Hutchinson, Fractals and Self Similarity, Indiana Univ. Math. J. 30(1981), 713-747.

U. REMBOLD: Autonomous mobile robots

In this paper the architecture and functions of an autonomous mobile system are described. For the operation of such a system knowledge-based planning, execution and supervision modules are necessary which are supported by a multi-sensor system. The individual functions of such a vehicle are explained with the help of an autonomous mobile assembly robot which is being developed at the University of Karlsruhe. The vehicle contains a navigator, a docking module and an assembly planner. Navigation is done with the help of a road map under the direction of the navigator. The docking maneuver is controlled by sensors and the docking supervisor. The assembly of the two robot arms is prepared by the planner and controlled by a hierarchy of sensors. The robot actions are planned and controlled by several expert systems.

C. M. HOFFMANN: Trade-Off between symbolic algebraic and floating point computation in solid modeling.

Solid modeling involves certain geometric operations such as surface/surface intersection evaluation. For example, given an intersection point, trace reliably the intersection curve and analyze its singularities. Can this process be made both reliable and efficient by combining techniques from algebraic geometry, Gröbner basis computation, and numerical approximation?

V. WEISPFENNING: Comprehensive Gröbner Bases

The Gröbner basis method initialized by B. Buchberger is a powerful tool for the algorithmic solution of many problems concerning multivariate polynomial ideals and their zeros in algebraically closed fields. It has, however, two significant drawbacks:

1. The construction of Gröbner bases is very sensitive to variations of the coefficients of the input polynomials.
2. While lexicographic Gröbner bases admit the computation of elimination ideals, they do not provide a necessary and sufficient condition on the coefficients of a system of polynomials in order that the the system has a common zero in the algebraic closure of the ground field.

Both problems can be overcome by the novel concept of a comprehensive Gröbner basis: Let K be a field, $R = K[U_1, \ldots, U_m, X_1, \ldots, X_n] = K[\underline{U}, \underline{X}]$ a polynomial ring over K. A specialization is a ring homomorphism $\varphi : K[\underline{U}] \to K' \supset K$ over K; φ extends cannonically to a ring homomorphism $\varphi : R \to K'[\underline{X}]$. Fix a termorder $<$ on $T(\underline{X})$. Then a finite set $G \subset R$ is a comprehensive Gröbner basis (w.r.t. $<$), if for all specializations $\varphi : K[\underline{U}] \to K' \supset K$, $\varphi[G]$ is a Gröbner basis (w.r.t. $<$) in $K'[\underline{X}]$.

Theorem 1 Given a finite set $F \subset R$ and a termorder $<$ on $T(\underline{X})$. Then one can construct a comprehensive Gröbner basis G w.r.t. $<$ such that F and G generate the dame ideal in R. For a suitable motion of a reduced comprehensive Gröbner basis G for F, G' is uniquely determined by the ideal $I(F)$ generated by F in R. Moreover, $\deg(G')$ and $|G'|$ are bounded by recursive functions in $\deg(F)$, $|F|$, m and n.

As a first application, we get:

Theorem 2 Let F be a finite subset of R and let G be a comprehensive Gröbner basis for $I(F)$ in R. Then G determines in an easy, explicit way boolean combinations $\delta_d(\underline{U})$ of polynomial equations $(-1 \leq d \leq n)$ such that for every algebraically closed $K' \supset K : \delta_d(\varphi(\underline{U}))$ holds in K' iff $\dim V_{K'}(\varphi(F)) = d$ for every specialization $\varphi : K[\underline{U}] \to K'$. (For $d = -1$, $\dim V_{K'}(\varphi(F)) = -1$ means $V_{K'}(\varphi(F)) = \emptyset$.)

The construction of comprehensive Gröbner bases can be extended to universal, comprehensive Gröbner bases, i.e. to work simultaneously for all termorders, and also to one- and two-sided ideals use the non-commutative polynomial rings of solvable type studied by Kandri-Rody & Weispfenning (J. Symb. Comp., to appear).

J. H. DAVENPORT: From Gröbner bases to solving equations

Many scientific areas have problems that can be expressed as the solution of polynomial equations. One particular area we have been working on is biochemistry. This talk will describe:

1. The scientific problem
2. The form of the Gröbner base
3. The conversion from this to a numerical solution that the scientists can understand.

We will also describe the use of factorization in Buchberger's algorithm, to produce solutions more rapidly.

H. J. STETTER: A computational algorithm for finding all zeros of a multivariate polynomial system

Let F be the ideal generated by the n polynomials $f_i : \mathbf{C}^n \to \mathbf{C}^n$. The construction of multiplication tables mod F for power products w.r.t. a power product basis permits the reduction of the root problem for the f_i to an eigenvalue problem for a set of matrices immediately defined by the multiplication tables: Each joint eigenvector of the (commuting) matrices contains all components of a (finite, isolated) joint zero of the f_i, and for each isolated zero of the polynomial system there is a corresponding joint eigenvector.
The algorithmic generation of the multiplication tables has been based on the results by Macauley and succeeds whenever the polynomial system has no zero manifolds of positive dimension (some open questions). If there are manifolds at infinity only, the algorithm may be modified appropriately. A numerical algorithm following this approach generates approximations for all isolated zeros of a multivariate polynomial system.

B. STURMFELS: Computational versions of the Quillen-Suslin-Theorem

We describe a constructive proof of the Quillen-Suslin theorem (Serre's conjecture) which computes an explicit free basis for a given projective $K(x_1, \ldots, x_n)$-module of finite rank. The resulting algorithm completes a unimodular polynomial matrix to a square invertible matrix. It can be implemented using Buchberger's Gröbner bases method. Applications include control theory and computational algebraic geometry. An independent alternative algorithm has been given by J. Heintz et.al. (1988). Using the effective Nullstellensatz, they give singly-exponential degree and complexity bounds. A combination of both methods with faster heuristics for special cases yields a practical algorithm for the Quillen-Suslin theorem.

KEN-ICHI KANATANI: Group theoretical methods in image understanding

The aim of image understanding is to extract, from $2D$ images, $3D$ information about the objects we are viewing - their sizes, locations, orientations, and motions in the scene. If an object model is assumed, the problem is estimation of model parameters from observations on images. If we define observable quantities of $2D$ images, we can derive, from the geometry of camera imaging, $3D$ recovery equations which relate the object model parameters with the image observables.

Since images do not have inherent coordinate systems, the choice of the observables must be essentially invariant to the rotation of the image coordinate system (invariance to $SO(2)$). It is also shown, from the camera imaging geometry, that the $3D$ recovery equations must be invariant to the rotation of the camera around the center of the lens (invariance to $SO(3)$). We discuss how to exploit such invariant properties by invoking the theory of Lie groups, Lie algebras, and their representations.

J. MUNDY: An Algebraic Basis for Modeling in Computer Vision

The use of geometric models as a basis for the recognition of three dimensional objects in two dimensional images has proven to be a practical and robust approach. Most experiments involve the use of fixed object models which are specified by numerical geometric data. In this talk we discuss the use of parametric object models which are represented as a system of geometric constraints. These constraints are expressed algebraically and the results are processed using a combination of symbolic and numeric manipulation. The symbolic processing is based on term rewriting methods. The numerical processing consists of standard non-linear optimization. The result is a new approach to object recognition based on systems of algebraic constraints.

S. S. ABHYANKAR: Invariant Theory

The discriminant of a quadratic equation is zero iff the two roots coincide. Changing the variable by a fractional linear transformation will change the roots but not their being coincidental. Hence it will not change the zeroness of the discriminant. In 1830 Boole confirmed this by showing that the discriminant gets multiplied by a non-zero quantity, namely the square of the determinant of the transformation. Cayley generalized this by defining invariants of univariate polynomials of any degree, or equivalently, invariants of bivariate forms of any degree. In 1865 Gordon proved that the invariants of a bivariate form are expressible in terms of a finite number of them. In 1890 Hilbert generalized this multivariate forms. Unlike Gordon's, Hilbert's proof was nonconstructive. Gordon's proof is based on what Young in his book on Invariant Theory (which he coauthored with Grace in 1902) has called the German Method or the Symbolic Method. The heart of this method is the FFT = the First Fundamental Theorem of Invariant Theory. The FFT says that invariants and covariants of any system of multivariate forms are expressible as meaningful symbolic expressions involving only dets and dots, i.e., determinants and dot products. The ideas of Clebsch, Gordon, Young, et.al., have culminated in the Straightening Law of Young Bitableaux which was formalized by Doubillet-Rota-Stein in 1972. Some of my own word in this direction may be found in my book entitled "Enumerative Combinatorics of Young Tableaux" published by Marcel Dekker in January 1988. Presently I am engaged in redoing this enumerative work by bijective methods obtained by modifying the RSK correspondence, i.e., the Robinson-Schensted-Knuth correspondence as explained in the third volume of Knuth's book on the Art of Computer Programming.

M. CLAUSEN: FFT

According to Wedderburn's Theorem the group algebra $\mathbf{C}G$ of a finite group G of order n is isomorphic to a suitable algebra of block-diagonal matrices. Every such isomorphism $W : \mathbf{C}G \to \bigoplus_{i+1}^{h} \mathbf{C}^{d_i \times d_i}$ is called a Fourier transform for $\mathbf{C}G$. Such a W links the convolution in $\mathbf{C}G$ and the multiplication of block-diagonal matrices. W.r.t. natural $\mathbf{C}$-bases, W can be viewed as an n-square matrix. The linear complexity of a matrix W is the minimal number $L_s(W)$ of $\mathbf{C}$-operations sufficient to evaluate W at a generic input vector. The linear complexity $L_s(G)$ of the finite group G is defined by $L_s(G) := \min\{\max(L_s(W), L_s(W^{-1})) \mid W \text{ a Fourier transform for } \mathbf{C}G\}$. Trivially, $|G| < L_s(G) < 2 \cdot |G|^2$, for any finite group. The classical FFT-algorithms improve the trivial upper bound by showing that for cyclic groups G, $L_s(G) = O(|G| \cdot \log|G|)$. Using Clifford theory, Beth (1984) showed that for soluble groups $L_s(G) = O(|G|^{\frac{3}{2}})$. Motivated by real-time applications in digital signal filtering we are interested in extending the FFT results to other classes of finite groups.

Theorem

1. $L_s(G) = O(|G|^{\frac{3}{2}})$
2. If G is metabelian (i.e. G has an abelian normal subgroup A with G/A abelian), then $L_s(G) = O(|G| \cdot \log|G|)$.
3. For symmetric groups $L_s(S_n) = o(|S_n| \cdot \log^3|S_n|)$.

The proofs "nearly automatically" translate into highly regular VLSI-designs.

D. JUNGNICKEL: The trace of primitive elements of $GF(q^m)$

The following theorem holds for all but finitely many pairs (q, k):

Theorem Choose an arbitrary element $a \neq 0$ in $GF(q)$. Then there exists a primitive element b of $GF(q^k)$ which has trace a over $GF(q)$.

In fact, there are at most 147 exceptional pairs (q, k), all with $k = 2$ and q odd. We conjecture that none of them is really exceptional. We also consider the analogous problem for trace 0.
Finally, the special case $b = 1$ and $k = 2$ is important in the construction of Costas sequences, as pointed out by Golomb in 1984.

Reference: D. Jungnickel & S.A. Vanstone: On primitive polynomials over finite fields, J. Algebra (to appear).

W. GEISELMANN: Selfdual Normal Bases over $GF(q)$

Starting with one normal basis $(b_0, \ldots, b_{n-1})$ of $GF(q^n) : GF(q)$ all normal bases can be constructed as $(b_0, \ldots, b_{n-1}) \cdot A$, where A runs over all invertible circulant $n \times n$-matrices over $GF(q)$. This well known method was transferred to orthogonal circulant matrices to calculate all selfdual normal bases ($SDNB$) if one is given. Due

to a paper of A. Lempel and M.J. Weinberger (1988) the problem of the existence of *SDNB*'s is solved in full detail for all finite fields.) By this method the number of all *SDNB*'s can directly be calculated for any finite field.

D. GOLLMANN: Multiplication in $GF(2^n)$

We examine the decomposition of multiplication into shift-and-add algorithms and the translation of these algorithms into hardware architectures for different basis representations. For polynomial basis representation we have two decompositions that correspond to serial input / parallel output multipliers. SIPO dual basis architectures follow from the same decomposition. The difference to polynomial basis architectures is only in the type of the linear feedback shift registers. Dual basis representations also allow PISO architectures. When the feedback polynomial is a trinomial we have a "weakly self dual polynomial basis" and these architectures also "accept" polynomial basis representations. For normal basis representation there is the PISO multiplier proposed by Massey and Omura. SIPO multipliers can be derived from a decomposition similar to the polynomial basis algorithms. Multiplication by the root of the feedback polynomial is the expensive step in all these normal basis architectures. It can be shown that PISO- and SIPO-multipliers are equivalent in this respect.

A. GUTHMANN: Constructive Arithmetic in $GF(q)[T]$

$p > 2$ a prime, q power of p, $\mathbf{Z}_T = GF(q)[T]$, $\mathbf{Q}_T = GF(q)(T)$, $\mathbf{R}_T$ = completion of $\mathbf{Q}_T$ w.r.t. degree valuation.
The following topics are discussed:

1. Extraction of square roots in $\mathbf{Z}_T$.
2. Continued Fractions in $\mathbf{R}_T$.
3. Divisors in $K = \mathbf{Q}_T(\sqrt{D})$, $D \in \mathbf{Z}_T$, and how to calculate with then.
4. The regulator group: Definition and formulas for addition.

H. H. NAGEL: Algebraic Approaches in Image Sequence Analysis

Image sequences, for example sequences of digitized video frames, allow to capture temporal variations in a scene. Algorithmic evaluation of such sequences aims at describing the $3-D$ (surface) structure of objects in the scene and their motion relative to the recording camera.
Given the coordinate vector $\vec{x1}_i$ at time $t1$ of the perspective image of a point $\vec{X}_i$ in space and the corresponding vector $\vec{x2}_i$ at time $t2$, these two entities are related by an equation $\vec{x2}_i^T E \vec{x1}_i = 0$ where the so called "essential matrix" E depends only on the translation $\vec{T}$ and rotation R between camera positions and orientations at times

$t1$ and $t2$. Various approaches towards the extraction of estimates for $\vec{T}$ and R from estimates of E are discussed.
Recent results by Demazure, Fangeras and Maybank (INRIA 1988) describe algebraic conditions for obtaining solutions for $\vec{T}$ and R.
Attempts to study the influence of measurement noise on the estimation of translation and rotation parameters result in challenging questions for algebraic approaches.

B. A. KUTZLER: Algebraic methods for automated geometry theorem proving

Implemented provers following the algebraic approach to automated geometry theorem proving are discussed. The basic idea of this approach is to translate a geometry theorem into an algebraic problem and to solve the latter by computer algebra methods.
After shortly explaining the technique how to obtain an appropriate algebraic translation of a geometry theorem, the three general purpose computer algebra methods, i.e. Collins' cylindrical algebraic decomposition method, Buchberger's Gröbner bases method, and Ritt's Characteristic sets method are investigated for their applicability to decide certain subclasses of geometry theorems. Explicit characterizations of what can be achieved by these methods as well as practical results on twenty representative examples are given. Then the provers of Wu, Chou, Kapur and Kutzler/Stifter, which are all based on Characteristic sets or Gröbner bases, are presented in detail and also applied to the twenty examples.
Finally, applications to constructive geometry and computer-aided design are sketched.

G. SCHIFFELS: Well Quasi Orders and Gröbner Ideal Bases

My talk is on joint work with *Andreas Dress*. We want to present a simple (but mainly *structural* and non-algorithmic) *approach* to the theory of *Gröbner bases* and some other *canonical bases* (e.g. by Szekeres, Re'dei, C. Ayoub). We proceed by introducing suitable *quasi-orders* $\preceq$ on the ground-ring K (commut. with 1), which are supposed to be *simplifying* for all K-ideals $\mathbf{a}$, i.e. each residue class $u + \mathbf{a}$ has a (unique) least element $\min_{\preceq}(u+\mathbf{a})$. For a commut. monoid $(\Gamma, +, 0)$, we consider the *monoid-algebra* $R = K^{(\Gamma)} = \sum_{\gamma\in\Gamma} K \cdot X^\gamma$, $X^\alpha \cdot X^\beta = X^{\alpha+\beta}$. In case $\Gamma = \mathbf{N}^{(I)}$ we have the polynomial ring $R = K[(X_i)_{i\in I}]$. For any partial order $\leq$ on Γ and the $\preceq$ on K, we introduce on $K^\Gamma(T)$ the *lexicographic quasi order* $\sqsubseteq$. If $\leq$ and $\preceq$ are *noetherian* or *well quasi ordered*, then so is $\sqsubseteq$. If moreover on Γ the relation $\exists\gamma : \alpha + \gamma = \beta$ defines a partial order $\alpha \leq_+ \beta$, and if $\leq$ is an addition-compatible well-ordered refinement of $\leq_+$, then $\sqsubseteq$ turns out to be simplifying for all R-ideals $\mathcal{A}$. For a basis A of $\mathcal{A}$, the appropriate *reduction* $\longrightarrow_A$ is noetherian, as $\sqsubseteq$ is. The basis A turns out to be *order-adapted* (i.e. *Gröbner*), iff for all $f,\ g \in R$ the relation $g = \min_{\sqsubseteq}(f + \mathcal{A})$ is equivalent to $f \to_A \cdot \to_A \cdots \to_A g$ and no $g \to_A h$. If $\leq_+$ is *well partial ordered* an K is a *noetherian ring*, each $\mathcal{A}$ has a *finite* Gröbner basis.
A preprint is available.

H. NIEDERREITER: The linear complexity profile of binary sequences

Stream ciphers are cryptosystems based on pseudorandom key streams, i.e. on deterministically generated sequences of bits with acceptable properties of unpredictability and randomness. From the viewpoint of cryptology a useful measure for unpredictability and randomness is the linear complexity profile of a sequence. It measures to what extent the initial segments of the sequence can be simulated by linear feedback shift registers. We present recent results on the linear complexity profile of binary sequences relating to the following problems:

(i) the construction of sequences with prescribed linear complexity profile;

(ii) the behavior of the linear complexity profile for truly random sequences.

The relevant algebraic tools are formal power series over finite fields and their continued fraction expansions. Applications to stream ciphers will be discussed.

D. E. LAZIĆ: Sphere Packing and Signal Constellations

There are many connections between the geometrical problem of packing equal spherical caps placed on the N-dimensional sphere Ω_N and the channel coding problem, i.e. the problem of design signal constellations for errorneous data transmission.
The long-standing Tammes problem of finding the densest packing of M equal sperical caps on Ω_N is analized. This problem can be viewed as equivalent to finding an arrangement of M points on Ω_N that maximize the minimal mutual distances between points. This arrangement $C_B(N,M)$ is called the best sperical code. It has important applications to the design of signal constellations for a band-limited channel with additive white Gaussian noise.
Using a method which consists of finding the minimum of a suitably chosen objective function of the codes distance distribution, all known conjectures for $C_3(3,M)$; $4 \leq M \leq 32$, are obtained, together with some solutions that are better than them. These solutions are expressed by means of Schlegel graphs and corresponding polytopes. Four-dimensional conjectures ale obtained for M ranging from 9 to 21 and for M=24 and M=25. In the higher-dimensional Euclidean spaces conjectures for the following best sperical codes are obtained:

$C_B(4,16)$, $C_B(5,13)$, $C_B(5,32)$, $C_B(6,16)$, $C_B(6,22)$, $C_B(6,64)$,
$C_B(7,25)$, $C_B(7,128)$, $C_B(8,40)$, $C_B(8,64)$, $C_B(9,64)$, $C_B(9,107)$,
$C_B(10,32)$, $C_B(10,101)$, $C_B(12,64)$, $C_B(15,32)$, $C_B(16,40)$, $C_B(17,51)$,
$C_B(18,64)$.

B. HAIBLE: Linear differential equations with polynomial coefficients

Let us call a power series f (in finitely many variables) differentiably finite (D-finite) if all its derivatives span an only finite-dimensional vector space over the rational functions. It is shown that D-finiteness is fulfilled for algebraic and elementary transcendental functions and preserved by addition, multiplication, Hadamard product

and diagonalization (taking the diagonal power series w.r.t. two of the variables). As an application, a canonical simplifier is presented for a huge subalgebra containing the elementary transcendental functions of the algebra of power series. As another application, it is shown that a wide class of sequences represented by sums that appear in combinatorics satisfy a linear recurrence relation with polynomial coefficients and therefore can be calculated fast.

K. MUROTA: LM-matrix and its combinatorial canonical form for systems analysis

Let K be a subfield of an extension field F. A matrix $A = \binom{Q}{T}$ is called a layered mixed matrix (LM-matrix) with respect to K if

(i) Q is a matrix over K, and

(ii) the nonzero entries of T are algebraically independent over K.

We show the fundamental properties of such a matrix, including its combinatorial canonical form, and discuss its role in the analysis of discrete systems such as electrical networks.

J. GRABMEIER: On sums of characters: zero-testing and interpolation

We reported on a joint work with A. Dress, Bielefeld ([DG 89]): Many ideas and methods from the recent papers on zero-testing and interpolation of k-sparse n-variate polynomials over fields of characteristic 0 ([BT 88]) and over finite fields $GF(q)$, q prime power, possibly allowing evaluations of elements from $GF(q^m)$. ([CDGK 88], [GKS 88]), can be unified and better understood by considering k-sums $\sum_{i=0}^{k-1} f_i\chi_i$ of characters $\chi_i : A \to (R,\cdot)$, where A is an abelian (semi-) group and R an integral domain with $f_i \in R$. The zero-test set

$$\left\{(z_0^T,\ldots,z_{n-1}^T) : T \subset \{0,\ldots,n-1\},\ \sharp T \le \lfloor log_2 n \rfloor,\ z_i^T = \left\{ \begin{array}{lll} 0 & \text{if} & i \in T \\ 1 & \text{if} & i \notin T \end{array} \right\}\right\}$$

of minimal size $\sum_{0\le i<\lfloor log_2 n\rfloor} \binom{n}{i} \sim n^{log_2 k}$ for $GF(2)$ from [CDGK 88] is constructed. Furthermore it is shown that finding elements that distinguish the involved characters, e.g. the method of [GKS 88] using Cauchy's determinants, together with appropriate zero-test sets are the essential ingredients for efficient interpolation algorithms.

[BT 88] Ben-Or, M., Tiwari, P.: A Deterministic Algorithm for Sparse Multivariate Polynomial Interpolation, Proc. STOC. ACM, (1988).

[CDGK 88] Clausen, M., Dress, A., Grabmeier, J., Karpinski, M.: On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields. Techn. Rep. TR 88.06.006, Heidelberg Scientific Center, IBM Germany, (1988).

[DG 89] Dress, A., Grabmeier, J.: On sums of characters, in preparation (1989).

[GKS 88] Grigoriev, D.Y., Karpinski, M., Singer, M.F.: Fast Parallel Algorithms for Sparse Multivariate Polynomial Interpolation over Finite Fields, preprint, (1988).

A. SHOKROLLAHI: Fermat Codes

V.D. Goppa's famous method of deriving linear codes from algebraic curves can be used to construct new and interesting classes of linear codes over finite fields. Utilizing the method of Goppa, one can construct codes on the Fermat curve $x^r + y^r + z^r = 0$ where $r = p^b + 1$ and the ground field is $\mathbf{F}_p^{2n}$. One problem which arises in this connection is that of determining a basis for the linear space $L(A)$ of some divisors A on the curve. Letting Q be the point $(\eta, 0, 1)$ where η is a primitive $2r - th$ root of unity in $\mathbf{F}_p^{2n}$ and fixing α with $2g - 2 < \alpha < n$ where g is the genius of the curve $(= \frac{1}{2}(r-1)(r-2))$ and n is one less than the number of the $\mathbf{F}_p^{2n}$-rational points on the curve, one gets: A basis of $L(\alpha Q)$ can be parametrized by the set

$$\left\{(a, b) \in \mathbf{N}_0^2 \mid 0 \leq b \leq \min(a-1, r),\ 0 \leq ar - b \leq a\right\}.$$

If C_α is the code attached to $L(\alpha Q)$ and $2g-2 < \alpha, \beta < n$ satisfy $\alpha + \beta = n + 2g - 2$, one has further

$$C_\alpha = C_\beta^\perp.$$

The computation of the exact minimal distance of these codes can be reduced to computation in the function field of the curve which has a very pleasent arithmetic behavior.

W. BÜTTNER: Modelling Complex Applications in Prolog

The term algebra used by Prolog to model domains of interest is inadequate when more exacting requirements have to be met as in modeling various phases of circuit design. Often, however, the structure of such a domain can be adequately described by a finite algebra. The characteristics of digital switching functions can be described, for instance, by a boolean algebra. It is outlined how the expressive power of Prolog can be amplified by an arbitrary finite algebra by implementing an equation solver operating with such an algebra. Implementations have shown the described procedures to enhance the expressive power and efficiency of Prolog to an equal extent.

J. CANNON: Knowledge-Based Systems as a Tool for Applied Algebra

Techniques from many areas of algebra, geometry and combinatorial theory are finding application to problems in physics, engineering and communications. Having chosen the appropriate mathematical theory, the applied mathematician will often need to get detailed information about a specific mathematical structure. For example, in many situations where groups are applied in physics, the physicist needs to know information about the characters of specific groups. It therefore makes sense to construct software systems which have the capability of answering many questions about specific algebraic and combinatorial structures. Such a system would contain

algorithmic knowledge, data bases incorporating families of critical examples, and possibly theoretical knowledge (definitions and theorems). A new version of the algebra system Cayley , designed to support computation in number theory, algebra and combinatorial theory, will attempt to integrate the use of all three types of knowledge.

A. KERBER: The combinatorial use of finite group actions

Whenever a mathematical structure can be defined as an equivalence class on a finite set, we can make effective use of the tools of finite group actions theory in order to enumerate, construct, generate ... such structures.
The basic tools, developed by Cauchy, Frobenius, Burnside and others were received and applied to symmetry classes of mappings. A particular example, the graphs, were discussed to some detail. Emphasize was laid on a redundancy free construction via double cosets and on a method that allows to generate orbit representatives uniformly at random.

Berichterstatter: W. Geiselmann

Tagungsteilnehmer

Prof. Dr. S. S. Abhyankar
Department of Computer Sciences
224, Computer Science Building
Purdue University

West Lafayette , IN 47907
USA

Dr. J. J. Cannon
Department of Pure Mathematics
The University of Sydney

Sydney N.S.W. 2006
AUSTRALIA

Prof. Dr. Th. Beth
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Haid-und-Neu-Str. 7

7500 Karlsruhe 1

Dr. M. Clausen
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Haid-und-Neu-Str. 7

7500 Karlsruhe 1

Prof. Dr. L. Budach
Forschungsbereich Mathematik/
Informatik der Akademie der
Wissenschaften der DDR
Rudower Chaussee 5

DDR-1199 Berlin

Prof. Dr. Zong-duo Dai
c/o Prof. Dr. Th. Beth
Fakultät für Informatik
Universität Karlsruhe
Postfach 6980

7500 Karlsruhe 1

Dr. W. Büttner
ZTI
Siemens
Postfach 83 09 53

8000 München 83

Prof. Dr. J. H. Davenport
School of Mathematical Sciences
University of Bath
Claverton Down

GB- Bath , BA2 7AY

Prof. Dr. J. Calmet
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Haid-und-Neu-Str. 7

7500 Karlsruhe 1

Dr. A. Dür
Institut für Mathematik
Universität Innsbruck
Technikerstr. 15

A-6020 Innsbruck

W. Geiselmann
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Haid-und-Neu-Str. 7

7500 Karlsruhe 1

B. Haible
Ritterstr. 42

7500 Karlsruhe 1

Dr. D. Gollmann
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Haid-und-Neu-Str. 7

7500 Karlsruhe 1

Dr. Ch. M. Hoffmann
Department of Computer Sciences
224, Computer Science Building
Purdue University

West Lafayette , IN 47907
USA

Dr. J. Grabmeier
IBM Deutschland GmbH
Wissensch. Zentrum Heidelberg
Tiergartenstraße 15

6900 Heidelberg

Dr. R. Janßen
IBM Deutschland GmbH
Wissensch. Zentrum Heidelberg
Tiergartenstraße 15

6900 Heidelberg

Dr. A. Guthmann
Fachbereich Mathematik
der Universität Kaiserslautern
Erwin-Schrödinger-Straße
Postfach 3049

6750 Kaiserslautern

Prof. Dr. D. Jungnickel
Mathematisches Institut
der Universität Giessen
Arndtstr. 2

6300 Gießen

H. Härtl
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Haid-und-Neu-Str. 7

7500 Karlsruhe 1

Dr. K. Kanatani
Department of Computer Science
Gunma University
1-5-1 Tenjin-cho

Kiryu 376, Gunma
JAPAN

A. Karst
Fachbereich Mathematik
der Universität Kaiserslautern
Erwin-Schrödinger-Straße
Postfach 3049

6750 Kaiserslautern

Dr. J. L. Mundy
Research and Development Center
General Electric

Schenectady , NY 12301
USA

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

8580 Bayreuth

Prof. Dr. K. Murota
c/o Prof. Dr. B. Korte, Institut f.
ökonometrie und Operations Research
Universität Bonn
Nassestr. 2

5300 Bonn 1

Dr. B. A. Kutzler
Institut für Mathematik
Universität Linz
Altenbergerstr. 69

A-4040 Linz

Prof. Dr. H. H. Nagel
Fraunhofer-Institut für
Informations- und Datenverarbeitung
Sebastian-Kneipp-Str. 10 - 14

7500 Karlsruhe 1

Dr. D. Lazic
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Haid-und-Neu-Str. 7

7500 Karlsruhe 1

Prof. Dr. H. Niederreiter
Kommission für Mathematik der
österreichischen Akademie der
Wissenschaften
Dr. Ignaz-Seipel-Platz 2

A-1010 Wien

Prof. Dr. H. Lüneburg
Fachbereich Mathematik
der Universität Kaiserslautern
Erwin-Schrödinger-Straße
Postfach 3049

6750 Kaiserslautern

Prof. Dr. U. Rembold
Institut für Prozeßrechentechnik
und Robotik
Universität Karlsruhe
Postfach 6980

7500 Karlsruhe

Prof. Dr. G. Schiffels
Fakultät für Mathematik
der Universität Bielefeld
Postfach 8640

4800 Bielefeld 1

Prof. Dr. H.J. Stetter
Institut für Angewandte und
Numerische Mathematik der
Technischen Universität Wien
Wiedner Hauptstraße 6 - 10

A-1040 Wien

Prof. Dr. M. R. Schroeder
III. Physikalisches Institut
Universität Göttingen
Bürgerstr. 42 - 44

3400 Göttigen

B. Sturmfels
RISC (Research Institute for
Symbolic Computation
Universität Linz

A-4040 Linz

M.A. Shokrollahi
c/o Mathematisches Institut II
Lehrstuhl Professor Leopoldt
Universität Karlsruhe
Englerstr. 2

7500 Karlsruhe 1

Prof. Dr. V. Weispfenning
Fakultät für Mathematik
und Informatik
Universität Passau
Innstr. 27, PF 2540

8390 Passau