Abstracts

Comunicaciones

(En *cursiva* los autores que está previsto que expongan)

(C1) V. Álvarez, *J. A. Armario*, M. D. Frau, P. Real

Estructuras algebraicas en modelos homológicos de grupos

Abstract

Homological Perturbation Theory has proved to be an efficient tool for designing a constructive approach in Homological Algebra. For instance, some algorithms have been given for computing (co)homology of some kind of groups and some implementations have already been achieved. The key for these (co)homological computations is to obtain "small" objects (resolutions or homological models) which allow to compute the (co)homology in a more economical way. Sometimes the differential operator of these homological models admits an elegant encoding as a twisted tensor product in the Brown sense. Algorithms for computing homological models for central extensions and semi-direct product of groups were designed. Here we investigate the algebraic structure of "twisted" tensor product on these homological models and give some ideas in order to see the importance of this study from a computational point of view.

(C2) J. Aransay, *J. J. Olarte*, J. Rubio

Implementación orientada a objetos de estructuras algebraicas: estudio de un caso en Java y C++

Abstract

The capabilities of Java and C++ for implementing algebraic structures are explored, in the particular case of semigroups and semigroup rings. Some limitations of these languages are detected and compared with the solutions designed using Common Lisp.

(C3) E. Artal Bartolo, *J. Carmona Ruber*, J. I. Cogolludo Agustín

Representaciones finitas del grupo de trenzas, monodromías de trenzas y topología de curvas algebraicas

Abstract

We find finite representations of the braid group and use them to effectively distinguish braid monodromies of affine curves. We apply this method to find a pair of curves with conjugate equations in a number field but which do not admit any orientation-preserving homeomorphism.

(C4) D. Assereto, *T. Moriarty*

Why you shouldn't even think of using Demonology in Cryptography: Some notes on Trithemius' Steganography

Abstract

Around 1499-1500 Tritemius, abbey of Spondheim, partially composed his book "Ste-

ganography" in which he was introducing several original ideas in cryptography.

However, considering essential that his revolutionary ideals were restricted to "learned persons" only, he disguised his book as a treatise of demonology; each "evocation" of demons which are the core of his book, were nothing else then an encoded version of his cryptographical algorithms; in his plan, the decoded version should have been teached in a cabalistical mood.

Unfortunately, Tritemius was publically attacked as a "conjurer" and he considered better to stop his project. As a consequence the book circulated as a manuscrypt only and the decoding secret was nearly lost when a printed version appeared in 1608, being immediately included in the "Index" and being still published today as a book of demonology.

A book explaining what it was behind the first two books of "Steganography" was published in 1624 (and went soon forgotten) while the content of the third book was decyphered just a few years ago. Having being forced to stop his project, Tritemius, still convinced of the importance of providing learned persons with a cryptographical tool to protect them from "imperitis Rapophagis" he wrote in 1518 a second book "Polygraphia" which had a wide diffusion.

The ideas introduced by Trytemius in "Steganography" and "Polygraphia" had a wide influence both in "classic" cryptography and (thru Agrippa and Caramuel) in the beginnings of combinatorics.

We are now working to an annotated version of Steganopraphy and the aim of this talk is to give a survey of Trytemius research. A preliminary version can be found in `http://www.disi.unige.it/person/MoraF/TESTO/aaa.html`

(C5) *M. Benito*, J. L. Varona

Aliquot sequences starting with a number under 10000

Abstract

In this paper we describe some advances in the knowledge of the behavior of aliquot sequences starting with a number less than 10000. We give the URL address of the web pages with the free number theory packages that we have used to compute the aliquot sequences up to their present status.

(C6) F. Botana, *J. L. Valcarce*

Obtención simbólica de lugares geométricos en el plano

Abstract

This paper describes a symbolic–dynamic geometry environment. Linking a dynamic geometry system and a computer algebra package, we have developed Lugares, a symbolic–dynamic program specialized in the obtaining of plane geometric loci.

(C7) J. M. Cabezas, *L. M. Camacho*, J. R. Gómez, E. Pastor

Mathematica y la clasificación de familias de álgebras de Lie en dimensiones concretas

Abstract

Using the package *Mathematica*, we present a program which aid in the obtaining of the classification of naturally graded 3-filiform Lie algebras of concrete dimensions.

(C8) *J. Carmona Ruber*

Aproximación numérica de trenzas algebraicas

Abstract

We describe an effective method to piecewise-linearly approximate an algebraic braid. This method can be implemented in Maple in order to obtain an algorithm that calculates certain topological invariants of an algebraic curve in $\mathbb{C}^2$, such as its braid monodromy and its fundamental group.

(C9) *B. Castaño*, J. Heintz, J. Llovet

Diferenciación automática de circuitos aritméticos: una implementación

Abstract

We describe an algorithm which computes all partial first order derivatives of a multivariate polynomial P given in arithmetic circuit representation. We introduce a suitable abstract data structure in order to implement such circuits and to evaluate them. Derivating the given circuit in a backward mode we obtain a new one which represents all partial first order derivatives of the given polynomial P. Experimental evidence shows that our implementation is more efficient than expected from theory.

(C10) F. J. Castro-Jiménez, *J. M. Ucha*

A computational approach to free divisors and logarithmic $\mathcal{D}$-modules

Abstract

We apply algorithmic techniques for comparing some $\mathcal{D}$-modules associated to a kind of divisors in $\mathbf{C}^n$.

(C11) S. T. Chapman, *J. I. García-García*, P. A. García-Sánchez, J. C. Rosales

Factorizations in atomic commutative monoids

Abstract

We present some characterizations of properties related with factorization problems on finitely generated commutative monoids. We also give a series of algorithms for studying these problems from a presentation of a given commutative monoid.

(C12) *F. Conde Torréns*

Método general de síntesis de mecanismos

Abstract

A new method for mechanisms design based on mathematics symbolic and numerical methods is presented in this paper. It allows the optimal design in several types of problems.

Here it is applied to the optimal design of a file-machine whit cinematic restrictions.

(C13) *C. D'Andrea*

Explicit Formulas for the Computation of Resultants

Abstract

We present formulas for computing the resultant of a family of sparse polynomials as a quotient of two determinants. These formulas extend the original formulation given by Macaulay for homogeneous polynomials.

(C14) E. Díaz, R. Fernández-Mateos, *D. Fernández-Ternero*, J. Núñez

An algorithm for classifying nilpotent Lie algebras of non-twisted affine type

Abstract

Every nilpotent Lie algebra of maximal rank is associated with an generalized Cartan matrix. This relation allows us to use the Kac-Moody algebras in order to classify the nilpotent Lie algebras of maximal rank. In this paper we give a classification method, in which we firstly need to obtain certain ideals of the positive root system of a Kac-Moody algebra and we also show an algorithm procedure which allows to obtain these ideals, up to isomorphism, when the generalized Cartan matrix is non-twisted affine.

(C15) *G. M. Díaz-Toca*, L. González–Vega

Cálculo de los desarrollos de Puiseux mediante el Lema de Hensel
y la Evaluación Dinámica

Abstract

This paper is devoted to show the use of Hensel Lemma and Dynamic Evaluation to compute the Puiseux expansions of a plane algebraic curve. First experimental results show a better behaviour than the classical methods based upon the Newton polygon.

(C16) *J. F. Fernando*, J. M. Gamboa

Polynomial images of $\mathbb{R}^n$

Abstract

We show that: (1) for any finite subset F of $\mathbb{R}^2$, the semialgebraic set $\mathbb{R}^2 \setminus F$ is a polynomial image of $\mathbb{R}^2$; and (2) for any independent linear forms $l_1, \ldots, l_r$ of $\mathbb{R}^n$, $n \geq 2$, the open semialgebraic set $\{l_1 > 0, \ldots, l_r > 0\} \subset \mathbb{R}^n$ is a polynomial image of $\mathbb{R}^n$.

(C17) *G. Fleitas Morales*

A computational study of the structure of Dwork matrices

Abstract

Let A be a Dwork matrix corresponding to a polynomial in several variables with coefficients in Z/p, p prime. We propose a method to compute the zeros of $det(I - At)$ mod. p^3, and the relationships among these zeros.

(C18) N. Franco, *J. González-Meneses*

Computation of the normalizer of a braid

Abstract

We give a new algorithm to compute the normalizer of an element of Artin's braid groups, based on an old algorithm due to Makanin, and on new techniques developed by Thurston and Dehornoy. The interest of this algorithm comes from a new Public Key Cryptosystem based on Artin braids.

(C19) *J. Gago-Vargas*

Bases de A_n-módulos proyectivos: algoritmos

Abstract

Let $R = A_n$ be the Weyl algebra. It is known that every projective finitely generated left module is free or isomorphic to a left ideal. Let M be a left module given as subset of a free module. In this paper we give an algorithm to detect if M is projective, to compute its rank, and if rank$(M) \geq 2$, to find a base. The last result depends on an effective version of a result of Stafford.

(C20) M. D. García Román, *M. S. García Román*

Un nuevo algoritmo para el cálculo de bases de Gröbner biláteras

Abstract

We give a new algorithm to compute a two-sided Gröbner basis of a two-sided ideal in every PBW algebra $R = k\{x_1, \ldots, x_n; Q, \preceq\}$ using the left Buchberger algorithm. This new algorithm improves the one already known since it calls only once the left Buchberger algorithm.

(C21) *Ph. Gimenez*

Cotas para la regularidad de Castelnuovo-Mumford de una curva tórica proyectiva

Abstract

Let $0 < \alpha_0 < \cdots < \alpha_{n-1} < d$ be an increasing sequence of positive integers such that $\gcd(\alpha_0, \cdots, \alpha_{n-1}, d) = 1$. Set $\mathcal{C}$ the projective toric curve in $\mathbb{P}^n_K$ parametrically defined by:

$$\mathcal{C} \;:=\; \{(u^{d-\alpha_0}v^{\alpha_0} : \cdots : u^{d-\alpha_{n-1}}v^{\alpha_{n-1}} : v^d : u^d) \in \mathbb{P}^n_K ;\, (u : v) \in \mathbb{P}^2_K)\}\,.$$

We give a combinatorial method to compute the Castelnuovo-Mumford regularity of $\mathcal{C}$, $\operatorname{reg}\mathcal{C}$, and deduce a simple proof of the inequality: $\operatorname{reg}\mathcal{C} \leq \deg\mathcal{C} - n + 2$.

(C22) R. González-Díaz, *P. Real*

An example in Combinatorial Cohomology

Abstract

Steenrod cohomology operations are algebraic tools for distinguishing non–homeomorphic topological spaces. In this paper, starting off from the general method previously developed for Steenrod squares and Steenrod reduced powers, we present an explicit combinatorial formulation for the Steenrod reduced power $\mathcal{P}_1^p : H^q(X; \mathbf{F}_p) \to H^{qp-1}(X; \mathbf{F}_p)$, at cocycle level, where p is an odd prime, q a non–negative integer, X a simplicial set and $\mathbf{F}_p$ the finite field with p elements. We design an algorithm for computing $\mathcal{P}_1^p$ on the cohomology of the classifying space of $\mathbf{Z}_p$ and we generalize this process to any simplicial set at cohomology level.

(C23) *E. González-Jiménez*, J. González

Curves of genus 2 parametrized from modular curves

Abstract

We prove that there are exactly 149 genus two curves C defined over $\mathbb{Q}$ such that there exists a nonconstant morphism $\pi : X_1(N) \to C$ defined over $\mathbb{Q}$ and the jacobian of C is $\mathbb{Q}$-isogenous to the abelian variety A_f attached to a newform $f \in\ S_2(\Gamma_1(N))$. We determine the corresponding newforms and present equations for all these curves.

(C24) *P. González-Pérez*, B. Teissier

Partial embedded resolution of non necessarily normal toric varieties

Abstract

We give a method to construct a *partial embedded resolution* of a non necessarily normal affine toric variety equivariantly embedded in a normal affine toric variety. This partial resolution is an *embedded normalization* inside a normal toric ambient space and a resolution of singularities of the ambient space provides an embedded resolution. The advantage is that this partial resolution is completely determined by any set of equations defining the embedding. As a by-product, the construction of the normalization is made without an explicit computation of the saturation of the semigroup of the toric variety. This result is valid for a base field K algebraically closed of arbitrary characteristic.

(C25) *J. Guàrdia i Rúbies*

Aplicaciones de los Thetanullwerte jacobianos

Abstract

We use the derivatives of odd hyperelliptic theta functions to solve polynomial equations of any degree. These formulas can be applied to solve in a completely effective way the hyperelliptic Torelli problem: recover an hyperelliptic curve from its jacobian. As an application of our explicit solution to the Torelli problem, we find rational equations of modular hyperelliptic curves.

(C26) *M. I. Hartillo*, N. Takayama, F. J. Castro-Jiménez

Some algorithmic questions on irregular hypergeometric D-modules

Abstract

We apply Gröbner basis computation on the Weyl algebra to calculate the slopes of some irregular hypergeometric systems.

(C27) *M. J. Jiménez*, P. Real

Estructura de Álgebra de Hopf en la 1–Homología de ciertas CDGAs

Abstract

Homological Perturbation Theory (HPT) provides an explicit description of both A_∞–algebra and A_∞–coalgebra structure $((m_1, m_2, m_3, \ldots)$ and $(\Delta_1, \Delta_2, \Delta_3, \ldots)$ respectively) for the 1–homological model H of a commutative differential graded algebra, A, (briefly CDGA). The A_∞–algebra structure is reduced, by using specific perturbation theory, to simple algebra structure. A_∞–coalgebra structure is much more complicated. In a previous paper we attacked the computation of Δ_2, and obtained an important improvement in complexity by using the Inversion Theory techniques. Here, we study this problem in some cases for which H is, actually, the 1–homology of A.

(C28) *J. S. Jorge*, J. L. Freire

Prove and then Execute

Abstract

In this paper, an example of developing and proving a functional program is shown. We introduce an experience in developing an applicaction in the area of symbolic computation, the computing of Grbner basis of a set of multivariate polynomials. Previous algorithms generally rely on informal methods that fail to establish its correctness. Our interest is that the program must be proved formally. This can be expedite by using functional programming properties as referential transparency.

(C29) A. Labajo Izquierdo, J. Martín Gómez, *A. Martín del Rey*

Aspectos computacionales del cálculo de los invariantes diferenciales de $y'' = F(x, y, y')$ usando Mathematica

Abstract

In this communication we implement the calculus of differential invariants of second-order ordinary differential equations using the mathematical software Mathematica$^{\mathrm{TM}}$ (version 4.0).

(C30) *A. Marco*, J. J. Martínez

Implicitación de superficies con ecuaciones paramétricas polinómicas

Abstract

An algorithm for computing the implicit equation of a surface possessing polynomial parametric equations is presented. It is based on an efficient computation of the multipolynomial resultant by means of classical multivariate polynomial interpolation. One of the main advantages of our approach is the fact that it considerably reduces the prob-

lem of intermediate expression swell, which is usually present in many computer algebra algorithms.

(C31) J. Miret, *R. Moreno*, D. Sadornil, J. Tena, M. Valls

Improvements of Goldwasser–Kilian primality test with elliptic curves $y^2 = x(x-1)(x-\lambda)$

Abstract

We study some properties and cryptographic applications of a family of elliptic curves over a finite field. The number of points of these curves is always a multiple of four and, conversely, for every multiple of four on the Hasse's interval, there exists a curve in our family with such an order. We compute the isomorphism classes of the family finding an explicit parametrization of them. Finally, we point out some improvements of Goldwaser–Kilian primality test by using the representatives curves of the isomorphism classes.

(C32) *M. A. Moreno Frías*

Gröbner δ-Bases. Applications: Flatness and Finiteness

Abstract

Let $\mathcal{H}$ be a noetherian sub-$\mathbf{k}$-algebra ($\mathbf{k}$ is a field) of the field $\mathbf{k}((X)) = \mathbf{k}((x_1, \cdots, x_n))$. We also suppose that $\mathcal{H}$ is stable under the action of the partial derivatives $\partial_1, \cdots, \partial_n$. Let us denote by $\mathcal{H}[\partial]$ the sub-$\mathbf{k}$-algebra of linear differential operators generated by $\mathcal{H}$ and $\{\partial_1, \cdots, \partial_n\}$. Let p be a prime ideal of $\mathcal{H}$. Given a non-zero left ideal I of $\mathcal{H}[\partial]$, the aim of this paper is to study, by using the Gröbner δ-bases theory, some effective results about the flatness of the $\mathcal{H}_p$-module $\mathcal{H}_p[\partial]/I_p$ and the finiteness of the $\mathcal{H}$-module $\mathcal{H}[\partial]/I$.

(C33) *M. Müller*, M. Clausen

An Efficient Computer Program for the Symbolic Construction of Irreducible Representations of Supersolvable Groups

Abstract

Baum and Clausen have presented an algorithm, refered to as BC-Algorithm, for the construction of a complete list of pairwise inequivalent ordinary irreducible representations for a given finite supersolvable group G. This algorithm is almost optimal in the sense that the running time is proportional to the length of the output up to some logarithmic factors. In this paper we describe an implementation, which realizes this algorithm for the first time efficiently concerning the running time as well as the memory requirements. Extensive tests have shown that the actual running time behaviour of the computer program reflects very well the theoretical complexity bounds. Furthermore, all arithmetic operations of the BC-Algorithm are done symbolically over $\mathbb{Z}/\mathbb{Z}_e$, where e denotes the exponent of G.

(C34) *I. Ojeda Martínez de Castilla*, P. Pisón Casares

Resolución envolvente de curvas monomiales en $\mathbf{A}^3(k)$

Abstract

In our work we study the hull resolution of a monomial curve in the three dimensional affine space. We compare it with the minimal free resolution of the monomial curve giving

a criterion for which the hull resolution is the minimal resolution in terms of the ideal of the monomial curve.

(C35) P. Pisón Casares, *A. Vigneron Tenorio*

Ideales de Lawrence y sus primeras sicigias

Abstract

A combinatorial characterization of the minimal degrees of a Lawrence ideal is given as well as a degree bound for its minimal first syzygies.

(C36) *P. Real*

Free resolutions for differential modules

Abstract

In this joint work with Tornike Kadeishvili, a free resolution $(R, d+h) \to (M, d)$ for a DG-module (M, d) over a DG-algebra (A, d) is constructed. The process is based in the perturbation of the differential on a free bigraded resolution $(R, d) \to M$ of the underlying graded module M over the underlying graded algebra A. As an application, an algorithm for computing a perturbation in the Koszul resolution of a field of characteristic 0 over a free commutative *differential* algebra is presented.

(C37) *E. Roanes Macías*, E. Roanes Lozano

Condiciones locales y globales para la determinación de lugares

Abstract

A method for determining geometric loci automatically, using Wu's algorithm (pseudo-division techniques), was recently developed by the authors. We have obtained new results later, finding necessary and sufficient local conditions for a point of the euclidean space K^n to be in the locus and also global conditions for an algebraic subvariety of K^n to be contained in the locus. These results, which include the case where more than one polynomial thesis exist, are shown here. Finally, these criteria are applied to determine a locus in an euclidean real space of dimension 3.

(C38) J. C. Rosales, *M. B. Branco*

Decomposition of a numerical semigroup as a intersection of irreducible numerical semigroups

Abstract

Every numerical semigroup S admits a decomposition $S = S_1 \cap \ldots \cap S_n$ with S_i irreducibles (that is, S_i is symmetric and pseudo-symmetric). We give lower and upper bounds for the minimal number of irreducibles in such a decomposition. We also study the problem of determining those numerical semigroups for which all S_i are symmetric, and when all S_i are pseudo-symmetric.

(C39) R. Rubio, *M. P. Vélez*

Análisis e implementación de un algoritmo de convexidad

Abstract

In this paper we recover an algorithm for convexity of sets defined as union of polyhedra. We present an implementation of this method in the Computer Algebra System Maple 6. This algorithm is polynomial in the number of polyhedra and variables; but it is exponential in the number of linear functions which describe the set.

(C40) *D. Sadornil*, J. Tena, P. Berrizbeitia

Factorización modular de ciertos polinomios ciclotómicos

Abstract

There are well known algorithm to obtain the factorization of the r-th cyclotomic polynomial, $\phi_r(X)$, modulo a given prime number p. We present a more efficient algorithm for the case when r is a Fermat prime, based only on the algorithm for computing square roots modulo p presented by Adleman, Menders and Miller. This algorithm will be used in a more general test to determine the primality of certain numbers of the form $p = Ar^n \pm 1$, $A < r^n$, r a Fermat prime. We implemented the algorithm for the cases $r = 5, 17$.

(C41) J. F. San Juan, A. Abad, *S. Serrano*

Una nueva formulación del método de Krylov–Bogoliubov–Mitropolski

Abstract

The Krylov–Bogoliubov–Mitropolski (KBM) method obtains asymptotic approximations to the perturbed harmonic oscillator. In this paper we develop a new formulation of the KBM method based on the Lie transformations that is better adapted to symbolic calculations than the original one. This method has been applied to the Earth and Mars cases of the artificial satellite problem.
