第一届全国计算机数学学术会议
报告摘要

大会邀请报告摘要

- **张景中院士，中科院成都计算所**

题目：微积分基础的新视角和计算机分析

摘要: 为微积分基础提出了一个新的数学模型，它和传统方法不同之处在于：

(1) 不依赖极限概念

(2) 导数和定积分是同一个模型

(3) 快捷展开推出主要定理

新的模型有望用于高等数学教育和分析中的自动推理。

- **李邦河院士，中科院系统所**

A determined algorithm for irreducible decomposition of algebraic varieties and primary decomposition of zero-dimensional ideal.

This is a joint work with Dingkang Wang and Fusheng Leng.

Let F be a polynomial set in $Q[x_1,\ldots,x_m]$, we can decompose F into a series of ascending chain $\{A_i\}$ given by polynomials irreducible over Q first. Then to get irreducible decomposition, we must decompose every A_i into irreducible ascending chains. Let $A=\{P_1,\ldots,P_n\}$ be an ascending chain with y_i be the leading variable of P_i, the other variables will be denoted by $u_1,\ldots,u_s$, so s+n=m. Let $K=Q(u_1,\ldots,u_s)$, then A is zero-dimensional ascending chain over K. Let d be the number of solutions of A. Substitute $y_1=y+a_2y_2+\ldots a_ny_n$ into A. We prove that among $(C_d^2)^{n-1}$ integral vectors $(a_2,\ldots,a_n)$ in (n-1)-cube $[b_1,b_1+C_d^2-1]\times[b_2,b_2+C_d^2-1]\times\ldots\times[b_n,b_n+C_d^2-1]$ with b_i integer, there must be

one $(a_2,\ldots,a_n)$ such that all ascending chains with polynomials irreducible over Q for the order $y < y_2 < \ldots < y_n$ are either with length <n or in the forms

$$Q_n(y, y_1,\ldots, y_n)$$
$$\ldots$$
$$Q_2(y, y_2)$$
$$Q_1(y)$$

$Q_2(y, y_2) = a_2(y)(y_2 + g_2(y))^{n_2} \ldots Q_i(y, y_2,\ldots, y_i) = a_i(y)(y_i + g_i(y))^{n_i}$

These new ascending chains give irreducible decomposition of A.

Besides, we can use only $(n-1)C_d^2 + 1$ also some special $(a_2,\ldots,a_n)$'s to arrive at the same aim. Our algorithm is used also to give primary decomposition of zero-dimensional ideal.

- **王文平教授，香港大学**

提目：Computation of Mesh Surfaces with Planar Faces

摘要：I shall discuss the problem of representing a free-form shape by a mesh surface with planar quadrilateral or hexagonal faces. This problem is motivated by the need in architecture for tiling free-form building surfaces with planar glass panels. Several effective modeling methods will be presented based on some novel concepts from discrete differential geometry, including conical meshes and Dupin duality. I shall also discuss the computation of offset and curvature of these discrete surfaces, and their connections to shape modeling of discrete constant mean curvature surfaces.

Joint Work with Yang Liu, Helmut Pottmann, Johannes Wallner and Alexander Bobenko

- **李洪波研究员，中科院系统所**

题目：从几何代数到高级不变量理论

摘要：微积分的发明人之一 Leibniz 有一个著名的梦想，希望能有一种几何计算可以直接处理几何体，而不是 Descartes 引入的一串数字（坐标）。他设想能有一种代数，它是如此接近于几何本身，以致于其中每个表达式都有明确的几何解释：或者表示几何体，或者表示它们之间的几何关系；这些表达式之间的代数运算，例如加、减、乘、除等，都对应于几何变换。如果存在这样一种代数，它可以被恰当地称为“几何代数”，它的元素被称为“几何数”。

在经典几何中，射影几何的几何代数是 Grassmann-Cayley 代数，仿射几何的几何代数是仿射 Grassmann-Cayley 代数，正交几何的几何代数是 Clifford 代数，而对于最常见的欧氏几何，满足条件“对几何体的表示具有协变性，几何体之间的乘法和除法在欧氏变换下具有等变性”的几何代数，只有近年来发展起来的共形几何代数才完全满足。

共形几何代数（CGA）不仅是欧氏几何，而且是几乎所有十九世纪经典几何的统一的几何代数。它由两部分组成：用于几何表示的共形 Grassmann-Cayley 代数，和用于几何变换的共形 Clifford 代数；前者通过 Grassmann-Cayley 代数运算，统一表示点、线、面、圆、球等的空间关联性质，后者通过 spin 群表示空间共形变换，能够将双向量 Lie 代数到 spin 群的指数映射替代以低次（二次或四次）多项式映射，对几何关系的表示和计算带来极大简化。

共形几何代数也为经典不变量理论从基本不变量发展到高级不变量提供了协变量代数基础。以基本不变量为核心的经典不变量理论，在 1970 年代由 Rota 学派复兴，以抽象括号表示基本不变量而不是以坐标和多项式系数为底层语言。在用于符号计算时，基本不变量代数依然遇到坐标表示遇到的几何解释困难、中间表达式膨胀两种主要障碍。只有高级不变量的引入和高级不变量理论的建立，才可能根本克服这些困难。

欧氏几何的高级不变量理论，由零括号代数（NBA）、零 Grassmann-Cayley 代数（NGC）、零几何代数（NGA）组成，通过零 Grassmann-Cayley 代数提供几何构造的长乘积表示，通过展开得到零括号代数中的长括号，以零几何代数作为长括号化简的核心工具。高级不变量理论的核心思想，是在变换和化简过程中，力求在中间的每一步都进行项数和次数控制，得到分解形式的和最短的结果。这种计算思想与传统的统一展开和标准化思想，在某种意义上恰好相反。

在经典几何的符号代数推理中，高级不变量理论有相当出色的表现。在测试的近百个困难欧氏几何定理中，三分之一以上只需要一项，只需要三四步简单操作就能够获证；绝大多数定理在两项之内可以完成证明，并通过减弱已知条件来加强定理结论的适用范围。这种出色的表现，本质上是高级不变量的几何代数基础和几何内蕴计算带来的结果。本报告将综述近几年来几何代数和高级不变量理论两方面的主要进展。

- **吴文玲研究员，中国科学院软件研究所**

题目：分组密码的研究进展

摘要：本报告首先介绍分组密码的研究意义、设计原理以及发展历史；其次简单介绍分组密码分析方法的研究进展，最后介绍我们课题组以不可能差分方法对三个标准分组密码算法的分析工作。

美国高级加密标准AES支持128、192和256比特三种规模的密钥，分别记为AES-128、AES-192和AES-256。由于AES的重要性，它的安全性分析引起了国际密码学界的广泛关注。几年来，国内外学者用各种方法分析AES的安全性，其中包括相关密钥攻击、积分攻击、不可能差分密码分析和代数攻击。目前对AES-128最好的分析结果有H.Gilbert和M.Minier给出的7轮碰撞攻击,其时间复杂度接近2^{128}.N.Ferguson和B.Schneier等人给出的7轮Square攻击,其数据复杂度为2^{128}-2^{119}.上述两个攻击方法都是近似强力攻击.我们利用不可能差分分析得到了对AES-128更好的攻击算法,其中数据复杂度为2^{115}、时间复杂度为2^{119}。提供攻击有效的关键点在于：（1）数据选取使用结构，降低数据量，（2）数据对的存储使用HASH表，降低计算量，（3）结合AES的子模块特性，对数据过滤做更多的限制，降低预测密钥比特时的时间复杂度。

ARIA是韩国的五个研究团队共同研制的一个分组密码，2004年被韩国商业、工业及能源部确立为韩国标准（KS X 1213）。ARIA的分组长度为128比特、密钥长度为128\192\256,

轮数分别为12、14和16.ARIA的整体结构采用的是SP结构,主要创新在于扩散层P的设计，扩散层P是ARIA实现性能良好的关键模块,并对ARIA的安全性有重要作用。设计者声称ARIA不存在4轮不可能差分，我们的研究表明ARIA存在4轮不可能差分，并进一步给出了6轮ARIA的不可能差分分析。此工作的意义在于指出设计者对一类扩散层P（包括相应32 x 32的构造方法）的错误认识，有利用相应密码算法的准确评估。

对于国际标准分组密码算法 Camellia，我们发现了 8 轮 Camellia 的若干不可能差分，并利用这些不可能差分对 Camellia 的安全性进行了分析。在密钥长度为 192/256 比特的情况下，攻击算法对 12 轮 Camellia 有效，这是目前可以攻击的最多轮数，我们的攻击算法比已有的攻击有更低的复杂度。提供攻击有效的关键点在于 8 轮不可能差分的发现，此工作的意义在于推进了对 Camellia 的安全性分析，加强了对一类密码结构的评估力度。

第 1 分组报告摘要

报告人：张树功

题目：多元多项式插值的 Newton 基

摘要：本文主要研究多元多项式插值的 Newton 基问题, 共分两个部分。第一部分针对多元 lower 子集上的 Lagrange 插值问题, 多元张量积格点集上的一致 Hermite 插值问题, 给出了极小次数 Newton 基以及 lower 子集的判别准则. 进一步, 我们提出了多元张量积格点的 tower 子集的概念,并给出了其上的 Lagrange 插值问题的极小次数 Newton 基.本文的另一部分是更加复杂的多元 Birkhoff 插值问题.我们提出了连通节点集和一般节点集的连通闭包的概念，通过构造相应的 Hermite 系统,给出了其上的 Birkhoff 插值 Newton 基.

报告人：Bo Yu And Bo Dong

Department of Applied Mathematics, Dalian University of Technology, Dalian, Liaoning 116024, China. (yubo@dlut.edu.cn).

Department of Applied Mathematics, Dalian University of Technology, Dalian, Liaoning 116024, China. (dongbodlut@gmail.com).

题目：A Symmetric Homotopy And Hybrid Method For Solving Mixed Trigonometric Polynomial Systems

摘要：Polynomial systems coming from mixed trigonometric polynomial systems have a special structure: the last *m* equations are *x*2 *n*+*i* + *x*2 *n*+*m*+*i* ¡ 1 = 0*; i* = 1*; : : : ;m*. And the *m* additional quadratic equations have an inherent symmetry. In this paper, exploiting the special structure and the symmetry, a symmetric homotopy is constructed and, combining homotopy method, decomposition and elimination techniques, an e±cient hybrid method for solving this class of polynomial systems is presented. Using the new hybrid method, some problems from the literature and a challenging practical problem are solved. Numerical results show that our method is much e±cient.

Key words. polynomial system, mixed trigonometric polynomial system, homotopy method, hybrid algorithm.

报告人：Liu Jinwang, li dongmei, Fu xiaoling

(College of Mathematics and Computation, Hunan Science and Technology University, Xiangtan, Hunan, 411201, China e-mail: Jwliu@hnust.edu.cn)

题目：The term orderings which are Homogeneouly Compatible with Composition

摘要：Let *K*[*x*1*,...,* *xn*] be the polynomial ring over a field *K* in variables*x*1*,... , xn*. Let $\Theta = (\theta_1, \cdots, \theta_n)$ be a list of *n* homogeneous polynomials in *K*[*x*1*,...* *,xn*]. Polynomial composition by Θ is the operation of replacing *xi* of a polynomial by θ_i. We say that

composition by Θ is homogeneously compatible with the term ordering > if for all terms *p* and *q*, *p* > *q deg p = deg q* implies that $p \circ lt(\Theta) > q \circ lt(\Theta)$. How to test it is very difficult, in this paper, we shall obtain a decision procedure for testing it; and obtain some important properties:

Proposition 1 Followings are equivalent

(i) $\forall p, \forall q, deg\ p = deg\ q;\ p > q \Rightarrow p \circ lp(\Theta) > q \circ lp(\Theta)$;

(ii) $\forall \vec{y} \in Z^n, \vec{y}$ is homogeneous, $\vec{y} \cdot A >_1 0 \Rightarrow \vec{y} \cdot T \cdot A >_1 0$.

Proposition 2 Followings are equivalent

(i) $\forall \vec{y} \in Z^n, \vec{y}$ is homogeneous, $\vec{y} \cdot A >_1 0 \Rightarrow \vec{y} \cdot T \cdot A >_1 0$;

(ii) $\forall \vec{y} \in Z^n, \vec{y} \cdot M \cdot A >_1 0 \Rightarrow \vec{y} \cdot M \cdot T \cdot A >_1 0$.

Proposition 3 Followings are equivalent

(i) $\forall \vec{y} \in Z^n, \vec{y} \cdot M \cdot A >_1 0 \Rightarrow \vec{y} \cdot M \cdot T \cdot A >_1 0$;

(ii) $\forall \vec{y} \in Z^n, \vec{y} \cdot B \cdot M \cdot A >_1 0 \Rightarrow \vec{y} \cdot B \cdot M \cdot T \cdot A >_1 0$.

Proposition 4 Following are equivalent

(1) $\forall \vec{y} \in Z^n, \vec{y} \cdot D \cdot M \cdot A >_1 0 \Rightarrow \vec{y} \cdot D \cdot M \cdot T \cdot A >_1 0$;

(2) the standard form $S = (P \vdots Q)$ of $(M \cdot A \vdots M \cdot T \cdot A)$ is a binary step matrix.

Proposition 5 The following are equivalent

(1) $\forall p, \forall q, deg\ p = deg\ q;\ p > q \Rightarrow p \circ lp(\Theta) > q \circ lp(\Theta)$;

(2) the standard form $S = (P \vdots Q)$ of $(M \cdot A \vdots M \cdot T \cdot A)$ is a binary step matrix.

报告人：Chen Yufu

Graduate University of Chinese Academy of Sciences

题目：Border Bases for Positive Dimensional Polynomial Systems

摘要：For the resolutions of zero dimensional polynomial systems, eigenvalue and eigenvector methods are effective. There border bases are needed and an efficiency algorithm to compute a border basis is important. In this talk we discuss how to generalize the border basis for the positive dimensional polynomial systems. We present the concept and give an efficiency algorithm to compute a border basis for a given polynomial system. The border bases can give more information on polynomial ideal, such as, dimension, maximum independent set, Hilbert polynomial, etc. But in this talk we present only an eigenvalue method to find some components of positive dimensional polynomial systems, which is based on the border bases.

报告人：支丽红、吴晓丽。
中科院系统所
题目：近似孤立重零点的精度优化

摘要： 提出基于 SNEPSolver 算法的符号数值算法，计算由复数域上一组多元多项式生成的理想的近似零点相关的准素分支，及零点的重数。由算法计算的对合基求出的乘法矩阵构造微分条件。利用微分条件构造单根系统，然后用经典的牛顿迭代方法提高根的精度。

报告人：邵莹

北京航空航天大学理学院，

题目：Wu-Ritt 特征列算法的验证实现

摘要：本文介绍在 Focal 系统中对 Wu-Ritt 特征列算法的验证实现．算法的验证实现是指在同一计算机系统中对算法进行形式化描述和证明所实现算法的正确性的过程．在软件设计中，对程序实现的过程进行形式化描述和在此基础上直接证明程序所需具有的性质被认为是一个有效的确保程序正确性的方法．

近年来，对算法的验证实现的研究取得了很多突破性的进展，例如 gcd 算法和 CAD 算法等都已在自动证明工具 Coq 中得到验证实现．这些算法都是在自动证明工具上得到验证实现的， 那么是否能在一个计算机代数系统中编写算法并验证其正确性？ Focal 的出现提供了这种可能性：它本身是一个计算机代数系统， 通过将 Focal 语言所编写的文件中的证明部分 由编译器自动转化为 Coq 语言提交到 Coq 进行验证来完成证明过程，结合了计算机代数系统和自动证明工具各自的优势．目前 Focal 的用户库中已经包括多项式环在内的代数结构和一些相关算法，更多内容正在补充中．

在 Focal 中进行验证实现时，首先需要对算法进行形式化描述，这个过程至关重要．

对数学对象描述的恰当与否会影响到计算的效率以及证明过程的繁简．Focal 程序中的证明部分是交由 Coq 完成的，由于 Coq 是一个基于归纳演算的证明工具，为了便于将来的证明

在形式化过程中我们尽量采用递归的方式描述算法； 在得到算法的形式化描述后，需要验证所实现算法的正确性．我们将验证每个数学对象被描述后满足相应的数学性质，只有确保形式化过程每一步的正确才能得到整个算法的正确性．为此，我们在 Focal 中编写每个所需性质的证明过程，然后利用 Coq 验证这些证明过程的正确性。

本文叙述我们对 Wu-Ritt 特征列算法进行验证实现的主要工作 ．其中算法的形式化过程已基本完成，主要包括对多项式及其相关运算、约化及伪除、 计算基列和特征列这三方面的描述.并且论述在此基础上展开的验证工作．如果能够证明算法中计算特征列的函数的输出结果 满足特征列定义中的三个部分(即函数输出结果是一个升列、 函数输出结果在输入多项式组所生成的理想中、输入多项式组对函数输出结果的伪余式集仅包含 0)，而且此函数能在有限步内终止，则我们认为算法得到了验证实现．此外，我们还将关注如何提高已验证算法的效率以及利用已形式化的内容发展其他算法的验证实现．

第 2 分组报告摘要

报告人：北京大学信息科学技术学院　许 超

题目：并行 JPEG2000 图像编码技术研究与数字电影系统设计

摘要：JPEG2000 图像编码标准采用一种高性能、但较为繁复的小波编码算法。基于目前的电子技术，实时 JPEG2000 图像编码只能通过并行编码技术、流水线式处理过程来实现，各个算法模块需要同步地工作。

JPEG2000 图像编码算法中的主要模块包括：小波变换模块、算术编码模块、率失真处理模块。本文基于前两年提出的并行 JPEG2000 图像编码技术，着重于整体编码系统结构的研究与优化，提出了与并行编码配套的逐点小波变换技术；提出了与并行编码配套的并行率失真处理技术；并形成了一套完整、优化的 JPEG2000 编码电路结构。而且，我们与中国数码集团和中国电影技术研究所合作，研制完成'基于 DCI 规范的数字电影播放原型系统'。DCI 规范是好莱坞的数字电影联盟发布的全球第一个数字电影行业标准。

逐点小波变换技术是使每一个小波变换系数的产生次序与后面的编码次序完全一致，而且，变换产生的小波变换系数与通常的小波变换系数的数值完全一致。其创新点在于：图像像素的 Z 形扫描方案的设计，与变换之中的中间结果的存储方案设计。图 1 为 Z 型扫描示意图。此设计不仅实现了与并行编码器的无缝衔接，而且存储器消耗也从 268K 下降到 60K。

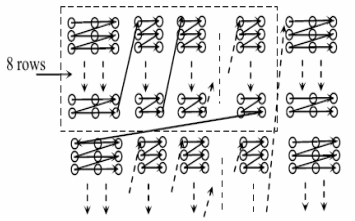


图 1、Z 形扫描图

率失真处理是对所有编码数据进行排序、输出的过程。主要操作是去除 RD 曲线上的凸点。如果等到所有数据产生后再进行处理，一要巨大的存储空间，二要极高的处理速度。我们分析发现，平均超过 85%的凸点是局部凸点。因此，设计了位平面并行处理方法去除位平面内的局部凸点，然后再利用简单的处理去除连接凸点。并行率失真处理结构与并行编码技术良好匹配，在编码性能上仅造成微小损失，一般 PSNR 下降小于 0.037dB。

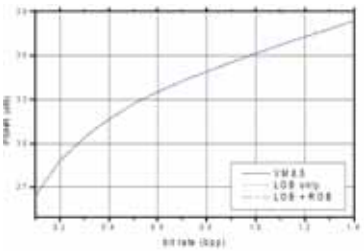


图 2、率失真曲线

逐点小波变换产生的每一个系数，被并行编码器接收，各比特立刻开始并行编码，编码数据被并行率失真处理器接收，计算率失真、去除局部凸点、进行排序后输出。如果要求较高，可以适量存储数据，进行率失真再处理，去除位间凸点，重新排序后输出。

另外，我们与中国数码集团、中国电影技术研究所，联合研发了基于 DCI 规范的数字电影播放系统。DCI 规范是在 2005 年 7 月发布的第一个数字电影行业规范，其中采用了 JPEG2000 作为数字电影图像的编解码方案。我们的工作主要是图像播放电路的设计。设计基于并行编码结构，利用了市场上现有的 ADV202-JPEG2000 芯片，三路并行解码，实现了 2K×1K 标准格式的数字电影的实时播放。

报告人：北京交通大学信息科学研究所 安高云　阮秋琦

题目：基于多尺度总体变分商图像的独立分量分析特征提取算法

摘要：在复杂背景的人脸识别任务中，光照条件的变化仍然是影响识别效果的一个重要因素，同时表情、年龄、拍摄距离、遮挡和化妆等外部干扰因素的影响也不容忽视。为克服这些外部干扰因素的影响，目前已经存在许多算法。其中，总体变分商图像模型(Total Variation based Quotient Image, TVQI)是解决光照影响的一个代表性算法。但是，现有 TVQI 模型在对复杂光照条件下人脸图像预处理过程中，仅保持和采用小尺度下的人脸特征作为具有光照不变性的识别特征。这些小尺度下的人脸特征虽然在小规模人脸库上表现出较高的光照鲁棒性，当被用于大规模人脸库(千人以上规模)的人脸识别任务时，这些小尺度下的人脸特征表现出较差的普适性，系统的整体性能较差。为解决这一不足，我们提出了一种"基于多尺度总体变分商图像的独立分量分析特征提取算法"。新算法主要包括如下三步：首先，结合特征融合技术和偏微分方程，新算法由原始图像提出和生成最佳光照不变性图像；其次，采用 Gabor 多尺度分析技术一方面对最佳光照不变性人脸图像进行多尺度分解以选取特定尺度和方向上的特征进行识别，另一方面对最佳光照不变性人脸图像进行升维操作以增加可识别或可鉴别的特征数目；最后，我们选用盲源分离领域的独立分量分析算法提取高阶统计量特征以用于选定的分类器进行识别。

本算法在识别率和整体性能方面要明显优于已有算法。尤其是在复杂背景下的人脸识别任务中，本算法在光照变化、表情变化、遮挡、化妆、年龄变化和拍摄距离变化六种条件下都表现出较高的鲁棒性。本算法还是一种适合单样本人脸库的人脸识别算法，从而可以减少采集和建设人脸库的成本和周期，进一步保证整个算法的实用性。

报告人：北京大学信息科学技术学院　张超

题目：红外人脸图像到可见光人脸图像的转换

摘要：提出了一种从红外人脸图像到可见光人脸图像的转换方法。通过典型相关分析的学习，可以把可见光图像和红外图像压缩到一个较低的维数，并且可以保证降维后数据的高相关性，通过线性回归分析得到二者的联系。然后把红外图像到可见光图像的转换过程看成超分辨率的过程，采用 LLE 的思想来学习一些新的信息，增加恢复的人脸的真实性。实验结果表明这一框架是可行的，这种方法保持了人脸的整体结构，并且从红外图像中获取了尽可能多的细节信息。

报告人：北京大学信息科学技术学院　罗定生

题目：基于空间覆盖的声学建模

摘要：声学模型建模的主要难点在于语音数据受多种因素影响而存在多种不同的差异，包括说话人，表达方式，语速，情感，口音及方言等，即语音数据的多变性(heterogeneous)，简单的混合训练(pool and train)方式会使声学模型的混淆度增大从而降低其识别性能，尤其在针对特定任务时其性能将比任务相关模型有较大下降。对训练数据进行归一化处理的方法有其局限性且不能保证在过程中语音内容的信息不受损失。建立基于知识的类别相关模型则存在数据稀疏和数据不平衡的问题，且在识别阶段需要对所属类别进行预先判断，这个步骤往往不够准确。

本研究基于空间覆盖的思想，在训练过程中采用数据驱动的方法，自动学习语音空间的子空间结构，使训练得到的模型概括而紧致，既覆盖整个语音空间又不失精确性。我们探索并实现了将状态分裂的方法引入声学模型训练过程中。在决策数据类後，选择并分裂方差，散度较大的状态，从而描述语音内容之外的各种差异，与以往方法相比，这种方法的特点是

完全是基于数据的。在建立基于数据的类别相关模型单元後，由于其单元更加细致，对轨迹的建模就更加重要。并引入概率浅语义分析（PLSA）的方法对训练数据中的单元共现进行统计建模，这种方法使得我们能够在训练数据中学习个单元的差异的一致性，其也是完全基于数据的。同时，从说话人差异着手，分析了由说话人导致的轨迹的差异，进而建立了概率说话人轨迹模型。实验结果表明，新框架下语音识别系统的性能得到良好的改善。

第 3 分组报告摘要

报告人：曹源昊 谢正 李洪波

题目：基于线性张量系统的微分几何定理的机器证明

摘要：我们提出了一个基于线性张量系统的微分几何定理机器证明的算法。首先，将微分几何定理的条件和结论转化成带指标的张量多项式；第二，利用规则重写、挖掘等价的 syzyy 和分次选取 syzygy 等方法，减少张量多项式系统的方程个数；第三，利用关于哑元的 syzygy 来三角化张量多项式系统；最后，将所得到的三角形式带入结论，得到定理的机器证明。这个算法已经在 Maple 10 上实现，利用它能够得到有难度的符号 n 维微分几何命题的可读机器证明。

报告人：Chunming Yuan

Key Lab of Mathematics Mechanization

Chinese Academy of Sciences

题目：Characteristic Set Method for Differential-Difference Polynomial Systems

摘要：In this paper, we present a characteristic set method for mixed differential and difference polynomial systems. We introduce the concepts of coherent, regular, proper irreducible, and strongly irreducible ascending chains and study their properties. We give an algorithm which can be used to decompose the zero set for a finitely generated differential and difference polynomial set into the union of the zero sets of regular and consistent ascending chains. As a consequence, we solve the perfect ideal membership problem for differential and difference polynomials.

报告人：陆征一

题目：Multiple limit cycles for three-dimensional Lotka-Volterra systems

摘要：It is well known that a two-dimensional Lotka-Volterra system cannot admit isolated periodic orbit; that is, if the system has periodic orbits, then these orbits are nonisolated. For dimension greater than or equal to three, in competition case, Coste et al. (1979) and Schuster et al. (1979) proved the existence of an isolated periodic orbit (limit cycle). Two limit cycles for a competition system were constructed by Hofbauer-So (1994) based on Hirsch's monotone flow theorem, the center manifold theorem, and the Hopf bifucation theorem. In their cases, the local stable positive equilibrium is surrounded by two limit cycles, in which one is from the Hopf bifurcation theorem and the other is guaranteed by the Poincare-Bendixson theorem. Multiple limit cycles were also constructed in three-dimensional Lotka-Volterra systems with various types of interactions formed by mutualism, competition and prey-predator by Lu-Luo (2002), Luo-Lu (2002) and Gyllenberg-Yan-Wang (2006).

In this talk, we classify the three-dimensional Lotka-Volterra systems into ten classes and show that besides the known results for classes 2, 4, 6 and 9, in each class of the remaining six ones, a system can be constructed to have at least two limit cycles based on the center manifold theorem and the Hopf bifurcation theorem.

报告人：王定康、孙瑶

中国科学院数学与系统科学研究院

数学机械化重点实验室

题目：参数椭圆曲线的 Zeta 函数的计算

摘要：根据 weil 猜想，椭圆曲线上的 Zeta 函数是一个有理函数。有限域中 Fq 上椭圆曲线的 Zeta 函数具有以下形式：

$$Z(t)=\frac{1-at+qt^2}{(1-t)(1-qt)}$$

其中 a 是需要确定的未知量。对于系数是参数的有限域 Fq 上椭圆曲线，我们将利用参数 Groebner 基的计算，将参数空间划分成互不相交的分区。在每一个分区上，计算出参数形式的 Groebner 基，在此基础上，给出其在 Fq 中有理点的个数，从而计算出它在每个分区上的 Zeta 函数。

报告人：马玉杰

题目：一类侵彻问题的模拟计算

摘要：对于一类侵彻问题，我们将问题转化后，转换为微分代数方程的混合计算。通过对这类问题的吴消元法处理，我们有效地进行了计算。在此基础之上，我们设计了自己的软件包，进行了相关部件的造型试算。我们利用自己的软件包计算得到了比 Prodase、LS-DYNA 及 Autodyn 2D/3D 更为精确的结果。与上述软件相比，我们的计算时间缩短了数个数量级，计算精度达到了可以实用的精度，并且我们的模拟计算及仿真结果与模型几乎一致。

报告人：陈奕俊

（华南师范大学数学科学学院　广东广州　510631）

题目：WZ 方法与一类含参变量积分的渐近估计问题

摘要：本文研究了利用连续的 WZ 方法来求一类形如 $\int_{a(x)}^{b(x)}F(x,y)dy$ 的含参变量积分当 $x\to x_0$（x_0 可为有限数或 $\pm\infty$）时的渐近估计的问题，基本的想法是利用下述本文所得的定理 2 将上述形式的含参变量积分的渐近估计问题转化成通常的定积分问题，而这一般来说都能得到解决或者可直接查阅积分表：

定理 2：若已知（$F(x,y),G(x,y)$）满足方程 $\frac{\partial F(x,y)}{\partial x}=\frac{\partial G(x,y)}{\partial y}$，且 $a(x)$、$b(x)$ 均关于 x 可导，令 $f(x)=\int_{a(x)}^{b(x)}F(x,y)dy$，则有下列公式成立：

$$f(x)=\int_c^x\left[F(t,b(t))\cdot b'(t)-F(t,a(t))\cdot a'(t)+G(t,b(t))-G(t,a(t))\right]dt+\int_{a(c)}^{b(c)}F(c,t)dt$$

其中c为某一适当选取的常数，且或者$a(x)$、$b(x)$在$x=c$处均无奇性且$\forall y\in R$，$F(x,y)$在(c,y)处均无奇性，或者$a(x)$、b（x）任一个在$x=c$处有奇性，或$\exists y_0\in R$使$F(x,y)$在(c,y_0)处有奇性，此时要求$\lim\limits_{x\to c}\int_{a(x)}^{b(x)}F(x,y)dy$存在且易求得，仍记此极限为$\int_{a(c)}^{b(c)}F(c,y)dy$。

同时我们还考虑了由下列方程$a_1(x)\dfrac{\partial F(x,y)}{\partial x}+a_0(x)F(x,y)=\dfrac{\partial G(x,y)}{\partial y}$构造一对 WZ 偶（$F'(x,y),G'(x,y)$）的问题，获得了下述本文的另一个主要结果：

定理 1：若（$F(x,y),G(x,y)$）满足方程$a_1(x)\dfrac{\partial F(x,y)}{\partial x}+a_0(x)F(x,y)=\dfrac{\partial G(x,y)}{\partial y}$，其中 $a_1(x)\neq 0$，令 $p(x)=-\dfrac{a_0(x)}{a_1(x)}$，$m(x)=\exp(\int p(x)dx)$，$F'(x,y)=\dfrac{F(x,y)}{m(x)}$，$G'(x,y)=\dfrac{G(x,y)}{a_1(x)m(x)}$，则可知（$F'(x,y),G'(x,y)$）构成一对 WZ 偶，即有$\dfrac{\partial F'(x,y)}{\partial x}=\dfrac{\partial G'(x,y)}{\partial y}$。

特别指出了针对上述两个问题，实际上$F(x,y),G(x,y)$可为初等函数，而不必限于为关于x、y的超指数函数，另外$a_0(x)$、$a_1(x)$也可为初等函数，而不必限于为关于x的多项式，从而可拓广连续的 WZ 方法所能解决问题的范围。

关键词：WZ 方法　WZ 方程　WZ 偶　含参变量积分　渐近估计

第 4 分组报告摘要

报告人：李 坚、梁延研、齐东旭

澳门科技大学资讯科技学院, 澳门

linxli3@yahoo.com, tonyleung.must@gmail.com, dxqi@must.edu.mo

题目：正交U&V系统在信号消噪及几何图组重构中的应用

摘要：本文研究一类新的正交函数系,包括一类早年(1983)建立的所谓“U-系统”,以及近年(2005)发展的所谓“V-系统”。它们分别可以看作是 Walsh 函数与 Haar 函数的推广。如同 Walsh 函数与 Haar 函数两者内在联系之自然,U-系统与 V-系统亦体现了彼此的互补与和谐。

勿庸置疑,正交函数及其变换算法,不仅是数学中极其优美的篇章,而且是解决信号处理重要实际问题强有力的工具。正交的概念古已有之, 特别在 Fourier 分析理论产生并发展了一套快速 Fourier 变换(FFT)的算法之后,使有关正交函数的研究显现其实用上的重要价值。

除了三角函数,其它正交函数系的丰硕研究成果不胜枚举。历史上,为了回答“是否存在非连续的完备正交函数系”的问题,Walsh 构造了后人称呼的 Walsh 函数(1923 年)。构造这类函数的初衷仅作为数学上的“反例”,然而它诞生了半个世纪后，因大规模集成电路的出现,才使这类只取值 1 或-1 的二值函数显示它的宝贵实用价值。

一方面,以正交函数方法为基础的频谱分析,在信号处理中成为不可或缺的手段。另一方面,在计算机辅助几何设计领域的数学模型中,尚欠缺直接用正交函数表达几何造型的研究。

几何模型正交表达的重要性在于:频谱分析手段可使复杂的二维及三维图组的整体特征得以生成,继而进行有效的分类与识别,而几何图组分类与识别的意义不言而喻。

这一研究的困难在于:通常的正交函数与正交变换用于几何造型表达与处理,难以避除 Gibbs 现象。如果说在诸如图象与语音的信号表达与处理中,Gibbs 现象的出现有时尚能接受,那么,对于诸如工程图与空间组合造型中产生莫名其妙的拓朴破坏,则是不可容忍的。

本文在信号处理中的消除噪声及几何造型的正交重构两方面,给出U&V-系统的实用算法研究。首先, 概述U&V系统及其若干变体;更着重介绍V-系统及其在三角域上的定义;继而提出多种三角域上V-系统函数生成元构作途径;提出了空间曲面片族的整体表达方法,给出曲面片族的“能量”计算公式,并附有例图。

针对典型的带噪声信号,提出了利用V-系统处理的新方案,并将V-系统处理的结果与已被认可的小波(db2、db4)及Slantlet方法处理结果作对比,检测数据表明,用V-系统处理可行、快速、精度提高明显。

关键词: U-系统, V-系统, 正交函数, 噪声消除, 几何重构.

报告人：汪国昭、徐岗、邓重阳

浙江大学 数学系计算机图像图形研究所 浙江 杭州 310027 wanggz@zju.edu.cn

题目：多项式参数极小曲面与 B 样条曲线升阶的研究

摘 要: 极小曲面是微分几何领域中一类非常重要的特殊曲面. 由于其优美的性质，它在建筑学、生物学、纳米技术、航海航空等领域都得到了广泛应用。但在计算机辅助几何设计

（CAGD）领域，极小曲面的研究才刚刚起步。

多项式参数曲面是 CAGD/CAD 系统中曲面形体表达的标准形式。作者从微分几何中一个经典结论出发，对多项式参数极小曲面进行了深入研究。首先分别给出了五次和六次多项式参数极小曲面的一个充分条件，然后基于该条件，构造出了几类带多个形状参数的多项式参数极小曲面，并对其性质进行了研究。通过研究发现，在低次多项式空间中，参数极小曲面存在并且具有类似的性质，如对称性、包含直线、自交性、存在共轭极小曲面等。最后，总结出任意次数情形下的一般规律，并提出了一个关于在多项式空间中极小曲面的存在性及其曲面性质的猜想。

由于极小曲面的高度非线性, 已有学者提出利用狄利克雷能量(薄膜能量)作为面积的一种近似, 以线性化极小曲面问题. 作者从平均曲率出发, 提出了极小曲面问题的一种新的近似能量函数. 与狄利克雷能量相比, 在某些情形下, 由该能量函数所产生的曲面能达到一种更好的近似.

B 样条的升阶，人们在八十年代就开始研究，升阶与割角的关系一直不明白，只知道升阶后的控制多边形的顶点是升阶前控制多边形顶点的凸线性组合。作者提出了双次 B 样条的理论：变 B 样条的升阶从整体升阶为逐段升阶，得到了升阶过程是割角过程的结论，即升阶前控制多边形按一定规律，经一次次割角后，可得到升阶后的控制多边形。

报告人：Guoliang Xu,　Dan Liu,　Qin Zhang

题目：Sixth Order Geometric Partial Differential Equations and Their Applications in Surface Modeling

摘要：Physics and geometry based variational techniques for surface construction have been shown to be advanced and efficient methods for designing high quality surfaces in the fields of CAD and CAGD. In this paper we derive a general sixth order geometric partial differential equation from minimizing a curvature integral functional. The obtained equation is used to solve several surface modeling problems such as free-form surface design, surface blending and N-side hole filling, with G^2 boundary constraints. We solve the equation numerically using a generalized divided difference method, where a quadratic fitting scheme is adopted to discretize several used geometric differential operators consistently. In computer aided geometric design and computer graphics, high quality fair surfaces with G^2 smoothness are sometimes required and important. The experiments show that the proposed method is efficient and yields high quality G^2 surfaces.

报告人：Zhaohui Guo, Jiansong Deng, Falai Chen, Xiaohong Jia

University of Science and Technology of China

题目：Proper Reparameterization of Rational Curves Using μ-Bases

摘要：An improper parameterization of a curve defines a many-to-one correspondence between the parameter values and the points on the curve. Hence the expression of the improper parameterization is redundant for tracing the curve more than once. Proper reparameterization presents the essential parametrization of the
curve by establishing a concise one-to-one correspondence between the parameter values and the points on the curve. This paper proposes a new efficient algorithm to compute the proper

reparameterization of planar curves. The algorithm makes use of the property of homogeneous function and the technique of computing μ-bases. Some examples are given to illustrate the new approach.

报告人：Ruixia Song

College of Sciences, North China University of Tech., Beijing, China

题目：On the V-system Over Triangular Domain

摘要：The V-system is a complete orthogonal system on $L_2[0,1]$. Comparing with the other orthogonal systems, the V-system has some distinctive characteristics: (1) The V-system is composed of smooth functions and discontinuous piecewise polynomials at multi-levels. (2) The V-system has multiresolution property and local support. (3) Using partial sum of the V-series, the geometric information expressed by piecewise polynomials can be precisely reconstructed without Gibbs phenomenon.（4）In the case of $k=0$ the V-system is just Haar system.

This paper further studies the V-system of two variables, The main contribution is to introduce the V-system of degree *k* defined over triangular domain for $k=0,1,2,3,\cdots$。

The V-system of degree k over triangular domain is constructed by groups and classes.

Firstly choose $\frac{1}{2}(k+1)(k+2)$ linear independent functions defined on triangular domain, using the Schmidt orthogonalization method to obtain orthonormal functions, which compose the first group of the V-system of degree *k*. We write it as

$$V_{k,1}^{i}(x,y),\quad i=1,2,\cdots,\frac{1}{2}(k+1)(k+2)$$

The second group of the V-system of degree *k* consists of $\frac{3}{2}(k+1)(k+2)$ piecewise polynomials of two variables of degree *k* (the generators ,must be constructed) defined on triangular domain under triangulation at level 1, denoted by $V_{k,2}^{i}(P), i=1,2,\cdots,\frac{3}{2}(k+1)(k+2)$.

The construction of *m*-th ($m=3,4,\cdots$)group of V-system of degree *k* is accomplished by performing squeezing and shifting operations on each of the generators, duplicating them into each of the sub-triangles under the triangulation at level *m*-2, set the function value 0 when *x* is outside the particular sub-triangle. The *m*-th group is divided into $\frac{3}{2}(k+1)(k+2)$ classes, and each class contains 4^{m-2} functions. $V_{k,m}^{i,j}$ denotes the *j*-th function in *i*-th class of *m*-th group of V-system of degree *k*, its expression is:

$$V_{k,m}^{i,j}=\begin{cases}2^{m-2}V_{k,2}^{i}(2^{m-2}(x-\frac{\beta-1}{2^{m-2}}),2^{m-2}(y-\frac{2^{m-1}-2\alpha}{2^{m-2}})), & (x,y)\in G_{\alpha,2\beta-1}\\ 0, & others\end{cases}$$

$$V_{k,m}^{i,j}=\begin{cases}2^{m-2}V_{k,2}^{i}(-2^{m-2}(x-\dfrac{\beta}{2^{m-2}}),-2^{m-2}(y-\dfrac{2^{m-1}-2\alpha+2}{2^{m-2}})), & (x,y)\in G_{\alpha,2\beta}\\ 0, & others,\end{cases}$$

$$m=3,4,\cdots,\ \alpha=1,2,\cdots,2^{m-2},\ \beta=1,2,\cdots,\alpha,\quad i=1,2,\cdots,\frac{1}{2}(k+1)(k+2),\ j=(\alpha-1)^2+\beta$$

报告人：徐东，刁麓弘，李宗民，李华

中国科学院计算技术研究所

题目：矩不变量研究及其在形状描述中的应用

摘要：矩不变量是一种由几何矩定义的描述几何形状特征的全局积分不变量，它与几何形状的旋转、平移、缩放等变换无关，可以用来描述物体的形状特征，以便进行匹配、识别和检索。

用距离、面积、体积等的基本几何不变量进行多重积分，获得了三维空间中任意阶数的矩不变量，并得到显式的有理多项式形式的表达式；将矩不变量定义推广到任意维空间（二维->三维->n 维），任意流形（线、面、体），和任意变换（相似、仿射、射影）；利用正交变换生成相位域，定义了相位矩不变量。

已经将相位矩不变量用于二维图像检索，矩不变量和欧氏距离变换相结合用于三维模型检索、曲线矩不变量用于蛋白质结构联配、公共子结构提取和结构检索以及分类等，显示了良好的应用前景。

第 5 分组报告摘要

报告人：王世坤

题目： 共形空间上的场方程

摘要： 本报告将介绍共形空间及其相关的一些数学问题和初步结果：（1） n 维 de Sitter 空间上 Yang-Mills 方程的整体解；（2）Dirac-L 空间的 Lorentz 度量、Dirac 场方程的解和拟共形度量；（3）共形 Pontrjagin 类和 Euler 类

报告人：费少明

题目： 量子纠缠的刻画和分类

摘要： 通过对代数不变量和几何不变量的计算，我们 给出了几类量子态在局域么正变换下的等价分类问题， 量子态集的所对应的微分流形及其度量结构。 对连续变量情形，我们研究了量子多模态所满足的不等式关系， 给出了量子多模态的一系列可分性条件。

报告人：张鸿庆

题目：数学机械化的基本原理

摘要：1.用机械化方法解方程， 2.用解方程的方法证明定理。

为完成这两项任务需要以下的基本原理：1 不变性原理，2.对偶性原理，3.协调性原理，4.本源性原理，5.奇正性原理。

用机械化方法解方程

解方程的一般模式： $Au=0 \xrightarrow{u=Cv} Dv=0$ (变易) ， $CKerD=KerA$ (不易)，选取简单的 D（简易）。

不变性原理：变易，不易，简易。选择简单的 C 和 D 使 $CKerD=KerA$。

对偶性原理：若 $CKerD \subseteq KerA$ 则 $\exists B$ 使得 $AC=BD$。

用这两个原理构造出一系列微分方程的解析解。

用解方程的方法证明定理

协调性原理：一生万象，万象协调，协调正合，正合归一。

证明定理的一般模式：

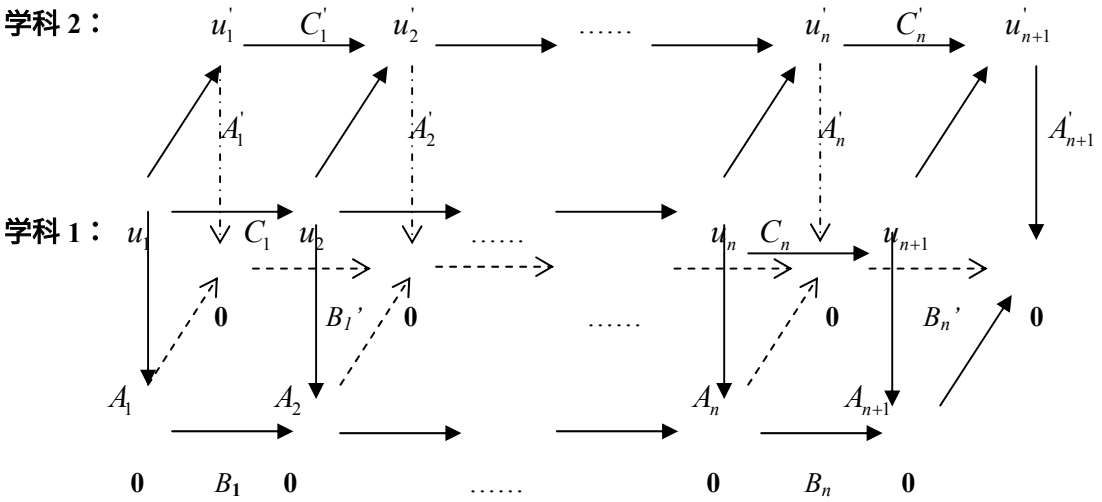
定义 1 → 定义 2 → …… → 定义 n-1 → 定义 n　　**定义链**

↓　　↓　　……　　↓　　↓

定理 1 → 定理 2 → …… → 定理 n-1 → 定理 n　　**定理链**

定义链和定理链相互对偶，定理链是定义链的伴随链。当箭头可逆时，上图构成一个交换正合图。用这个模式可以证明一系列的定理。

学科间的映射（同构，同态，……）：



一. 半机械化

本源性原理：明示根本，指解源流，正本清源，温故知新。

奇正性原理：道可道，非常道，不可道为奇，可道为正。

我们用这两个原理对泛函分析等学科研究了这些学科产生的规律。

报告人：李志斌

题目：Automated derivation of the Backlund transformations for a class of nonlinear PDE

摘要： A direct and algorithmic method for constructing a kind of auto Backlund transformations (BT) is proposed. And a Maple package named AutoBT, which can entirely automatically generate auto BT is presented, the effectiveness of AutoBT is demonstrated by applications to a variety of nonlinear evolution equations with physical interest as examples. Not only are previously known BT relations recovered but in some cases new or more general form of BT relations are obtained.

报告人：闫振亚

题目：A family of (N+1)-dimensional generalized NLS equations: similarity transformations and spatiotemporal solitons

摘要：In this paper, a family of (N+1)-dimensional generalized nonlinear Schrodinger (NLS) equations is investigated. Firstly, we make a similarity transformation to reduce this family of equations to a family of nonlinear ordinary differential equations with constant coefficients and a system of nonlinear partial differential equations. Secondly, we solve these two families of nonlinear determined equations using some ansatze, respectively. Finally, many types of solutions of the family of (N+1)-dimensional generalized NLS equations are derived. In particular, for the case N is greater than 1, these obtained solutions

contain arbitrary functions which generate abundant structures and are useful to explain some physical phenomena.

报告人：Yonggui Zhu

School of Science, Communication University of China, Beijing 100024, China

题目：New exact solitary-wave solutions with compact support for the K(2,2,1) and K(3,3,1) equations

摘要：In this paper, the Adomian decomposition method is employed to find the solitary solutions for K(2,2,1) equation: $u_t + (u^2)_x + (u^2)_{xxx} + u_{5x} = 0$ and K(3,3,1) equation: $u_t + (u^3)_x + (u^3)_{xxx} + u_{5x} = 0$. New exact solitary solutions with compact support are developed by the symbolic computation system, Maple.

第 6 分组报告摘要

报告人：冯克勤　清华大学

题目：对称布尔函数的代数免疫性

摘要：为了抵抗流密码和分组密码中的代数攻击，需要寻求具有最佳代数免疫度的布尔函数。对于对称布尔函数，我们引进重量支持集概念和判别代数免疫度的一个简化引理。由此在算法、计数和构作三方面都得到新结果。

报告人：Rongquan Feng, Hongfeng Wu

School of Mathematical Sciences, Peking University

题目：Efficient Arithmetics on Elliptic Curves over Fields of Characteristic 3

摘要：Efficient elliptic curve arithmetic is crucial for cryptosystems based on elliptic curves. Such cryptosystems often require computing kP for a given integer k and a curve point P. For example, if k is a secret key and P is another user's public key then kP is a Diffie-Hellman secret shared between the two users. So a main operation for elliptic curve cryptosystems is the point multiplication: $Q = kP$, where the multiplier k is generally a secret (or private) parameter. Many methods to speed up this operation have been actively studied.

A non-supersingular elliptic curve over a field of characteristic 3 has a point of order three if and only if it can be written in the form $y^2 = x^3 + x + b$ or equivalently the Hessian form $x^3 + y^3 + 1 = Dxy$. In this talk, new point multiplication algorithms in two forms: Weierstrass and Hessian forms are presented. These algorithms are more efficient than the best known algorithms in elliptic curves over fields of characteristic 3. Moreover, efficient and secure point multiplication algorithms based on the Euclid addition chain and the double-base chain, and the unified additions formulae are also given. These algorithms can protect against the side-channel analysis.

报告人：林东岱　中科院软件所

题目：分布式/并行化密码计算技术

摘要：近些年来，在计算机技术和网络技术飞速发展的推动下，计算技术、计算工具和计算平台都发生了巨大变化，出现了符号计算、网络并行计算与网络分布式计算等一些计算新技术。怎样将这些新的计算技术和新的计算工具应用于密码计算对提高我国的密码设计和密码分析能力将有重要的意义。我们根据密码计算的特点提出了一种通用的分布式密码计算模型，设计了一种面向服务的体系结构，利用网格提供的基本服务，将网格计算引入密码计算中，成功开发了使用互联网环境的通用分布式密码计算网格系统平台。该平台是一个可分布在多台计算机上、通过互联网互相协同进行密码计算的通用平台，测试表明，计算性能提高

明显，为我们通过有限的计算资源，提高密码计算能力提供了一种有效的方法。

报告人：Chunming Tang[1]　Zhuojun Liu[2]　Dingyi Pei[1]

1 School of Mathematics and Information Sciences, Guangzhou University, China(510006)}

2 Key Laboratory of Mathematics Mechanization, CAS, China(100080)

题目：Efficiently Cryptographic Primitive from ∑-protocols*

摘要：In this paper, we will construct the following cryptographic primitive based on ∑-protocols if one-way function exists:

1：interactive witness indistinguishable and witness hiding protocols for any NP;

2：non-interactive witness indistinguishable and non-interactive witness hiding protocol for any NP;

3：non-interactively perfectly hiding and computationally binding commitment scheme.

Comparing with existed works, items 1 and items 2 were constructed from ∑-protocol on Hamiltonian Cycle and ∑-protocol for relation OR, however, they are constructed only from ∑-protocol on Hamiltonian Cycle in this paper. In FOCS2006, STOC2006, STOC2007, a perfectly hiding and computationally binding commitment scheme was constructed under the existence of one-way functions respectively, however, all of them have polynomial number of rounds, i.e., impractical. Our works will be the first work to construct practically perfectly hiding and computationally binding commitment scheme under the existence of one-way function.

Keywords: Cryptography, witness indistinguishable, witness hiding, ∑-protocol, perfectly hiding and computationally binding commitment scheme.

报告人：邓映蒲 中国科学院数学与系统科学研究院

题目：代数免疫度为 1 的布尔函数

摘要：给出代数免疫度为 1 的布尔函数的 Walsh 谱刻画，指出变量个数大于 2 的 Bent 函数的代数免疫度不为 1；给出代数免疫度为 1 的布尔函数的精确计数公式；给出代数免疫度为 1 的布尔函数的非线性度的紧的上界。

报告人：Xiao-Shan Gao, Fengjuan Chai, and Chunming Yuan

Institute of Systems Science, Chinese Academy of Sciences

题目：A Characteristic Set Method for Solving Boolean Equations and Applications in Cryptanalysis of Stream Ciphers

摘要：We present a characteristic set method for solving polynomial equation systems in the finite field F2. Due to the special property of F2, the given characteristic set methods are much more

efficient and simpler than the general characteristic set method. In particular, we could give an explicit formula for the number of solutions for a given polynomial equation system. We can also prove that the well-ordering principle can be executed in a polynomial number of steps in terms of the number of variables. We also use our methods to solve equations raised from cryptanalysis of stream ciphers based on nonlinear filter generators. Extensive experiments show that our method is comparable with the best implemented Groebner basis method for a large set of problems.

第 7 分组报告摘要

报告人：曾振柄、杨路、郭远华

题目：通过数值计算得到一个几何最优化问题的符号解

摘要：本报告讨论如下一个几何最优化问题。设已知椭圆的长半轴和短半轴分别为 a,b，又设 L 是内接于这个椭圆的所有三角形的周长的最大值。求 L,a,b 满足的公式。这个问题，首先可以根据周长取到最大值的三角形的一个几何性质，把三角形的自由度从3减少到1。然后利用Lagrange乘子法求这个单参数三角形族的最大周长。这时对应的代数问题是从形状如下的一组多项式

$$f_0(L,a,b,t_1,t_2,t_3)=0, f_1(a,b,t_1,t_2,t_3)=0, f_2(a,b,t_1,t_2,t_3)=0, f_3(L,a,b,t_1,t_2,t_3)=0$$

消去变元 t_1,t_2,t_3 得到 $R(L,a,b)=0$。然后分析 $R(L,a,b)$ 的哪一个不可约分支满足原来的几何问题。消元可以采用伪除法、结式或者Groebner基。例如，可按如下格式先消去 t_3:

$$g_0=\text{resultant}(f_0,f_1,t_3), g_1=\text{resultant}(f_2,f_1,t_3), g_3=\text{resultant}(f_3,f_1,t_3),$$

然后对得到的结果做因式分解并剔除那些明显不符合几何意义的因子（如下面的 t_1-t_2, g），

$$g_0=g_{01}\cdot g_{02},\quad g_1=(t_1-t_2)\cdot g^3\cdot g_{11}(a,b,t_1,t_2),\quad g_2=8\cdot g^2\cdot g_{21}(L,a,b,t_1,t_2),$$
$$(g=b^2(1-t_2^2)^2+4a^2t_2^3)$$

再按如下格式消 t_1,t_2:

$$h_0=\text{resultant}(g_{01},g_{11},t_1)\cdot\text{resultant}(g_{02},g_{11},t_1),\quad h_1=\text{resultant}(g_{21},g_{11},t_1),$$
$$R=\text{sqfree\_resultant}(h_0,h_1,t_2),$$

这里的函数sqfree_resultant 表示先作无平方因子分解再算结式（如此可以简化计算）。

如果计算过程都能实现的话，那么这个问题也没有任何特别了。可是，在这个具体问题的计算中，h_0 的计算在一个有 $2GHz$ Xeon CPU和 $2GB$ 内存的工作站上用了18,000 秒完成了，而 h_1 用了1,497,240 秒（约17天零7小时）还没有得到结果。直接用Dixon结式消元也没有成功。

本报告讨论如何用数值计算和符号计算结合解决所讨论的优化问题。我们得到的最后结

果是：

$$L=\frac{2\sqrt{3}b^2}{\sqrt{a^2+b^2+2\sqrt{a^4+b^4-a^2b^2}}}+2\sqrt{2a^2-b^2+2\sqrt{a^4+b^4-a^2b^2}}\ ,$$

我们在报告的最后也要列出另外一些未解决问题，希望可能推广本文的方法得到它们的答案。

报告人：南昌大学数学系　　曾广兴

题目：多元实有理函数的连续性之有效判定

摘要：在微积分的大多教科书中，判定多元实有理函数在分母零点（即分母作为多项式的零点）处的连续性是一类有代表性的习题。否定某个实有理函数在分母零点处的连续性，传统的方法是让函数的自变量坐标点沿不同路径趋向分母零点处，使得函数值沿不同路径获得各自不同的极限。该方法的关键在于不同路径的巧妙选择，而这种路径的选择总是因题而异，缺乏一定的规律性可循，有点叫人妙不可言。至于函数连续性的肯定，似乎只有藉助定义通过所谓的 “ε-δ”语言来获得证明。由于任意给定的正数 ε 实际上仅是一个符号，从而为得到 δ 的某个满足要求的且依赖 ε 的表达式往往颇费心计。

我们的研究目的，正是寻求一个能够判定多元实有理函数在分母零点处的连续性的有效方法。

设 $\boldsymbol{f(x_1,...,x_n)}$ 和 $\boldsymbol{g(x_1,...,x_n)}$ 是实数域 $\boldsymbol{R}$ 上两个 n 元多项式，$\boldsymbol{(a_1,...,a_n)\in R^n}$，使得 $\boldsymbol{g(a_1,...,a_n)=0}$。对于取定的一个实数 $\boldsymbol{b}$，可规定如下实函数：

$$\Phi(x_1,...,x_n)=\begin{cases}\dfrac{f(x_1,...,x_n)}{g(x_1,...,x_n)}, & 若 g(x_1,...,x_n)\neq 0\\ b, & 若 (x_1,...,x_n)=(a_1,...,a_n)\end{cases}$$

面临的问题是：如何有效地判定函数 Φ 在点 $\boldsymbol{(a_1,...,a_n)}$ 处的连续性？

根据问题的实质，我们的研究工作如下：

(1) 通过 Collins 的柱形代数分解，给出了一个有效方法，判定如下极限是否存在：

$$\lim_{(x_1,...,x_n)\to(a_1,...,a_n)}\frac{f(x_1,...,x_n)}{g(x_1,...,x_n)}。$$

这里，我们的方法有别于通常的柱形代数分解，所获得的样本点全为有理点。从而避免实代数数的运算。

（2）在极限存在时，给出了上面的极限的一个有效计算方法。

（3）在极限存在的情况下，对于代表任意正数的符号 ε，获得了一个有效方法，用来产生适合 “ε-δ”语言的一个 δ 的显性表达式。明确地说来，若上面的极限被计算为 A，则对于代表任意正数的符号 ε，可有效地获得一个 δ 依赖于 ε 的显性表达式，使得

$$\text{当}(x_1-a_1)^2+\ldots+(x_n-a_n)^2<\delta\text{时，恒有}\left|\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}-A\right|<\varepsilon\text{。}$$

为获得这样一个有效方法，我们应用了赋值论和实域论的相关知识。

报告人：符红光，赵世忠

中科院成都计算机应用研究所

题目：Dixon 结式的多余因子

摘要：Dixon 结式是一种基本消元方法，它在机器人等高技术领域中有着重要应用. 但是由于结式方法可能产生多余因子，因此多余因子的产生机理一直是一大难题，目前还没有一个在 Dixon 结式构造过程中去掉多余因子的通用算法. 最近，我们根据 Dixon 结式在原多项式系统理想中的表示形式，发现 Dixon 结式的多余因子主要由 Dixon 导出多项式的多余因子，Dixon 矩阵的多余因子以及导出多项式回代产生的多余因子三大部分组成，并给出了一个在 Dixon 结式构造过程中去掉多余因子的通用算法。

报告人：侯晓荣、邵俊伟

电子科技大学　宁波大学

题目：球面五点如何分布时其距离和最大？

摘要：球面上 5 个点如何分布时，它们之间 10 个距离之和最大？这个问题公开已有半个世纪了。有不少文章论及该问题，但都只是给出一些相关问题的解答；提到该问题时，仅给出猜测的结果：5 点是双金字塔结构（赤道均匀分布 3 点，南北极各 1 点），都没有给出严格的数学证明。利用我们提出的基于区间分析的不等式自动证明的方法，我们给出了该猜测的一个严格证明。所用的机器是 PC Intel Pentium IV 2.0GHz, RAM 512M，软件是 Maple11，用时 791331.803 秒（约 9.16 天）.

报告人：Yong-Bin Li

School of Applied Mathematic

University of Electronic Science and Technology of China

题目：Some further property of triangular sets

摘要：Let K be a field of characteristic 0 and $K[x_1,\ldots,x_n]$ the ring of polynomials in the variables $x_1,\ldots,x_n$ with coefficients in K. Suppose that

$$\mathbb{T}=[f_1(u_1,...,u_r,y_1),f_2(u_1,...,u_r,y_1,y_2),\cdots,f_s(u_1,...,u_r,y_1,...,y_s)],$$

where $(u_1,...,u_r,y_1,...,y_s)$ is a permutation of $(x_1,...,x_n)$, is a triangular set in $K[x_1,...,x_n]$. The following important assertion proved by Aubry et al. in 1999 (other proof given by Wang in 2000): $\mathbb{T}$ is a regular set （introduced by Yang and Zhang in 1991 and Kalkbrener in 1993） if and only if $sat(\mathbb{T})=\{p\in K[x_1,...,x_n]\,|\,prem(p,\mathbb{T})=0\}$ can be deduced from the result $Ideal^*(\mathbb{T})=\{p\in K(u_1,...,u_r)[y_1,...,y_s]\,|\,prem(p,\mathbb{T})=0\}$ where $Ideal^*(\mathbb{T})$ stands for the ideal generated by all elements of $\mathbb{T}$ in $K(u_1,...,u_r)[y_1,...,y_s]$, obtained by Yang et al. in 1996. Furthermore, we present that $\mathbb{T}$ is also a Grobner basis of $Ideal^*(\mathbb{T})$ if $\mathbb{T}$ is a normal triangular set (or p-chain introduced by Gao et al. in 1992).

According to the analytic method established by Zhang et al. in 1991, the U-set of $\mathbb{T}$ (denoted by $\mathbb{U}_{\mathbb{T}}$) which is usually more simple than the set of initials of $\mathbb{T}$. $\mathbb{U}_{\mathbb{T}}$ has the following useful property $Zero(\mathbb{T}/\mathbb{U}_{\mathbb{T}})\subseteq Zero(sat(\mathbb{T}))$ (presented by author in 2006) . Furthermore, we prove that $Zero(sat(\mathbb{T}))=Zero(Ideal(\mathbb{T}):U^{\infty})$ where $Ideal(\mathbb{T})$ stands for the ideal generated by all elements of $\mathbb{T}$ in $K[x_1,...,x_n]$ and $U=\prod_{u\in\mathbb{U}_{\mathbb{T}}}u$, this result develops the assertion $Zero(sat(\mathbb{T}))=Zero(Ideal(\mathbb{T}):V^{\infty}),\ V=\prod_{v\in ini(\mathbb{T})}v$ (obtained by Wang 2000). Based upon the above results, we give a note on improving the unmixed decomposition for the variety (introduced by Gao et al. in 1993).

报告人：王云诚，方伟武，吴天骄

题目：An algorithm of global optimization using cut-peak functions

摘要：An algorithm is proposed for finding a global minimizer of a multimodal function with multiple variables. The basic idea of the algorithm is described as follows: Constructing a so-called cut-peak function and a choice function for each present minimizer, the original problem of finding a global solution is converted into an auxiliary minimization problem of finding local minimizers of the choice function, whose objective function values are smaller than previous ones. For a local minimum solution of auxiliary problems this procedure is repeated until no new minimizer with a smaller objective function value could be found for the last minimizer. Construction of auxiliary problems and choice of parameters are relatively simple, so this algorithm is relatively easy to implement, and the results of the numerical tests are satisfactory compared to the filled function methods. As an application, the algorithm is also used for finding zeros of nonlinear functions and proved more satisfactory.

第 8 分组报告摘要

报告人：王东明（北京航空航天大学、法国科学研究中心）

题目：几何学的形式化与机械化

摘要：有关几何学机械化的已有工作主要在于定理的机器证明、几何计算和交互式几何作图. 这里我们提出一个将几何学形式化和机械化的框架. 其核心思想是使用基于带有嵌入知识的谓词和函词的逻辑语言，将几何知识（包括对象、关系、定理、问题等）完全形式化，建立形式化的几何知识库. 以此为基础，我们设计并实施各种软件模块来动态管理几何知识文档，进行符号几何计算、定理自动证明、自动或交互式几何作图与问题求解，从而更全面地实现几何研究、教学和应用的机械化. 我们将介绍上述框架的结构和内容，并报告我们的工作进展.

报告人：廖启征 北京邮电大学

题目：串联机械手的倍四元数求解与并列机构位置正解中的一些问题

摘要：

用倍四元数解决空间串联机械手的反解问题:

Cliford 代数中当 $C^{+}(0,4,0)$ 时，可以导出（Double quaternion），我们称之为倍四元数。国外,倍四元数已经应用到了刚体的空间位姿的插值和一些机构的综合当中。最近我们利用倍四元数对串联机械手进行正反解建模及求解获得成功。我们参考倍四元数进行插值的建模方法，首先把 4×4 的齐次坐标变换矩阵近似变为 4×4 的空间 4 维旋转矩阵，然后把它与倍四元数对应起来，就构成了描述机械手位移的倍四元数形式的封闭方程。然后展开为 8 个结构和形式相同的方程，经过线性消元和 Dixon 结式消元，我们完成了三类 6 自由度串联机械手的位置逆解，包括 6R、1P5R、4R1C 三种机构。目前该方法还不完善，还存在计算中需要提取若干公因式的问题。

广义并联机构理论研究

高小山提出的广义 Stewart 并联机构当中，具有 CCS 运动链的机构，其位置正解相对比较复杂。从高的研究结果来看，每增加一个 CCS 运动链，减少一个 SPS 运动链，整个机构正解的次数就要增加一倍。按照这一想法，我们曾对 5SPS-1SPC 广义并联机构位置正解进行研究，发现它是 80 次的，与 6SPS 的 40 次刚好是 2 倍。在此基础上，我们对台体型 4SPS-2SPC 广义并联机构位置正解进行了研究。首先基于四元数建立了位置正解的数学模型，然后应用同伦连续法进行了数值演算，在 PC 机上，跟踪了 1 024 条路径，运行 1 003 秒，得出该机构全部的 160 组位置正解，数字计算表明高小山证明的该机构位置正解的最高上限 160 次是可以达到的。

到目前为止，我们已经完成了 5SPS-1CCS、4SPS-2CCS、3-CCC、6-CCS、3D3A、4D2A 等几种广义并联机构的位置正解。

平台型并联机构的研究：

此外，我们还改进了吴文达先生的一项工作，即 6-6 平台并联机构位置正解，它是平台型并联机构中最复杂的一种。我们的方法是，首先基于计算机符号运算，运用分次字典序 Groebner 基，从 6 个基本方程出发，推导出 15 个只含 3 个变量且最高次数为 4 次的多项式方程组，然后构造结式，从而导出该问题的一元 20 次方程。研究发现，15 个方程不是唯一的，不需要求出约化 Groebner 基，只需要找出包含待求解多项式方程组所有首相理想的多项式方程，即可构造出相应结式，从而推导出一元高次方程。该方法与 Bucherberg 算法相比，不需要对 S-多项式的每一项进行约化，因此可以节省计算机运算时间，同时构造出的 15 个方程也相对简单，计算效率要稍微高一些。

报告人：黄文奇　叶涛

华中科技大学 计算机学院　武汉 430074

题目：求解等圆最紧布局问题的完全拟物算法

摘要：美国大数学家 R.L.Graham 用 20 余年的时间，组织和吸引了近百名很有特色的数学家研究了等圆 packing 问题。其哲学目的是要尝试着求解 NP 难度问题。

在初始的酝酿阶段为了推动他的研究工作以及检验他的工作成效，他需要寻找一个非常天然的明白的 NP 难度问题作为他的思考的介质和靶子。几年后他终于 找到了等圆 packing 问题。

二三十年后的今天，等圆 packing 问题成了国际上校验 NP 难度问题的求解性能的最天然的试金石。用此试金石一试即可大致试出各种哲学(算法)是属于 上、中、下等中的哪一等，是属于忠实的哲学呢还是属于泡沫的哲学。

确切地说，等圆 packing 问题是问在平面上如何尽量紧密地放置 n 个半径为 1 的圆饼，紧密性的度量是这放好了的 n 个圆饼的外包装圆的半径 Rn，Rn 越小越好。

经过 20 余年的努力，在今天，R.L.Graham 及其近百名的师友与学生研制出了许多不同的算法，对于每一个具体的 n(n=1,2,3,...,100)，他们联合起来都得到了一个他们认可的最好结果——n 个圆饼的布局图象及其相应的外包装圆的半径 Rn。

我们的工作结果是得到了一个唯一确定的统一算法，利用此算法对这 100 个 n 值分别进行了计算，作出了相应的布局，最后打破了 Graham 学派所保持的世界纪录中的 6 项纪录，即对于 n=66,67,70,71,77,79 找到了更好的布局图案，将相应的包装圆的半径 Rn 缩小了十万分之一至百万分之一：10-5~10-4。

我们所用的方法是改进的拟物方法，即当拟物算法陷入局部极小值陷阱时，就天然地引进高强度的引力与斥力，迫使各个圆饼作剧烈的运动以使计算跳出 陷阱走向前景更好的地方。

原始的拟物算法的不足之处在于计算陷入局部极小值陷阱时就无能为力了，需要调用拟人策略。然而拟人策略的制定又颇费时力，有时还难免带有一些人为的性质。

在改进的拟物算法中，计算点的下降与跳坑都是拟物，所以可被称之为完全的拟物算法。

报告人：杨立波

题目：A Major Index for Matchings and Set Partitions

摘要：For a permutation $\pi=a_1a_2...a_n$, a pair (a_i, a_j) is called an **inversion** if $i < j$ and $a_i > a_j$. The statistic $inv(\pi)$ is defined as the number of inversions of π. The **descent set** $D(\pi)$ is defined as $\{i: a_i > a_{i+1}\}$, whose cardinality is $des(\pi)$. The sum of the elements of $D(\pi)$ is called the major index of π (also called the greater index) and denoted $maj(\pi)$. One of the classical results on permutations is the equidistribution of the statistics *inv* and *maj*. A statistic equidistributed with *inv* is called **Mahonian**.

Given a partition of $[n]=\{1,2,...,n\}$, there is a natural generalization of inversions, namely, *2-crossings*, which can be viewed easily on a graphical representation of the partition. In this paper we introduce a new statistic, called the *p-major index* and denoted *pmaj(P)*, on the set of partitions of $[n]$. We prove that for any $S, T\subseteq[n]$ with $|S|=|T|$, *pmaj* and *cr_2*, the number of 2-crossings, are equally distributed on the set $P_n(S, T)$. Here $P_n(S, T)$ is the set of partitions of $[n]$ for which S is the set of minimal block elements, and T is the set of maximal block elements. Restricted to permutations, the pair $(cr_2, pmaj)$ coincides with (inv, maj). This generalizes MacMahon's equidistribution theorem for the permutation statistics.

报告人：李树荣　张晓东

（中国石油大学(华东)信息与控制工程学院，东营, 257061）

题目：聚合物驱提高原油采收率的最优控制模型及求解

摘要：针对聚合物驱提高原油采收率的最优开发决策问题建立了最优控制模型，性能指标为一定时间内原油开采所获得的利润，约束方程为渗流力学偏微分方程组。对于该最优控制问题，提出了一种基于控制向量参数化的数值求解方法，利用分布参数系统最优控制的必要条件来计算性能泛函的梯度，并且针对流量和井底压力的约束问题提出了一种新的处理方法。通过一个二维聚合物驱最优问题的计算实例表明了所提出求解方法的有效性。

报告人：Yongwei WU, Chen Gang, Guangwen YANG, Weimin Zheng

Department of Computer Science and Technology;

Tsinghua National Laboratory for Information Science and Technology

题目：Grid Scheduling based on Prediction of Task Completion Time

摘要：Scheduling problems of grid research area are paid more and more attention recently. In this paper, a grid Scheduling model based on Prediction of task Completion Time (SPCT) is proposed.

Through Using Least Squares Discrete Curve Fitting, SPCT dynamically establishes the regression function of Completion Time of Task (CTT) according to the historical record first. Predicted Completion Time of each coming task is calculated for each candidate node with the regression function secondly. And then, the node with the least value will be allocated to run the task.

The SPCT is used to input data sensitive applications and implemented in one real-world grid environment, Bioinformatics Grid Platform. Experimental result shows that the SPCT could reduce the average CTT of tasks by 19%.