25 Years of SINGULAR

talk at the

AIMS

-

Gerhard Pfister

pfister@mathematik.uni-kl.de

Departement of Mathematics

University of Kaiserslautern

SINGULAR

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

A Computer Algebra System for Polynomial Computations

with special emphasize on the needs of algebraic geometry, commutative algebra, and singularity theory

SINGULAR

A Computer Algebra System for Polynomial Computations

with special emphasize on the needs of algebraic geometry, commutative algebra, and singularity theory

W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann
Technische Universität Kaiserslautern
Fachbereich Mathematik; Zentrum für Computer Algebra
D-67663 Kaiserslautern

A Computer Algebra System for Polynomial Computations

with special emphasize on the needs of algebraic geometry, commutative algebra, and singularity theory

W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann

Technische Universität Kaiserslautern

Fachbereich Mathematik; Zentrum für Computer Algebra

D-67663 Kaiserslautern

The computer is not the philosopher's stone but the philosopher's whetstone

Hugo Battus, Rekenen op taal 1983

Birth of SINGULAR

- 1984

History

1983

Greuel/Pfister: Exist singularities (not quasi-homogeneous and complete intersection) with exact Poincaré-complex?

1984

Neuendorf/Pfister: Implementation of the Gröbner basis algorithm in basic at ZX-Spectrum

History

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

1983

Greuel/Pfister: Exist singularities (not quasi-homogeneous and complete intersection) with exact Poincaré-complex?

1984

Neuendorf/Pfister: Implementation of the Gröbner basis algorithm in basic at ZX-Spectrum

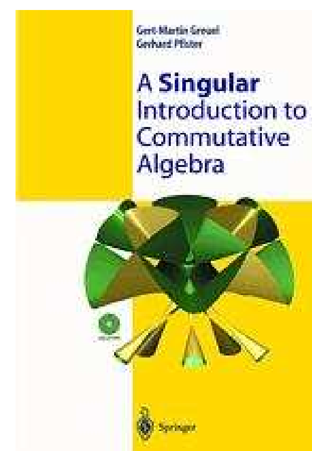
History

1983

Greuel/Pfister: Exist singularities (not quasi-homogeneous and complete intersection) with exact Poincaré-complex?

1984

Neuendorf/Pfister: Implementation of the Gröbner basis algorithm in basic at ZX-Spectrum



2002

Book: A SINGULAR Introduction to Commutative Algebra (G.-M. Greuel and G. Pfister, with contributions by O. Bachmann, C. Lossen and H. Schönemann).

History

2004

Jenks Price

for:

Excellence in Software Engineering

awarded at ISSAC in Santander

History

2004

Jenks Price

for:

Excellence in Software Engineering

awarded at ISSAC in Santander

http://www.singular.uni-kl.de

History

2004

Jenks Price

for:

Excellence in Software Engineering

awarded at ISSAC in Santander

http://www.singular.uni-kl.de

- Supported by: Deutsche Forschungsgemeinschaft, Stiftung Rheinland-Pfalz für Innovation, Volkswagen Stiftung
- SINGULAR is free software (Gnu Public Licence)

Team

T. Wichmann, C. Lossen, G.-M. Greuel, H. Schönemann, W. Pohl, G. Pfister, V. Levandovskyy, E. Westenberger, A. Frühbis-Krüger, Oscar, K. Krüger

Team

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

T. Wichmann, C. Lossen, G.-M. Greuel, H. Schönemann, W. Pohl, G. Pfister, V. Levandovskyy, E. Westenberger, A. Frühbis-Krüger, Oscar, K. Krüger

Kaiserslautern
Saarbrücken
Cottbus
Berlin
Mainz
Dortmund
Valladolid
La Laguna
Buenos Aires

surfaces: http://www.imaginary2008.de/

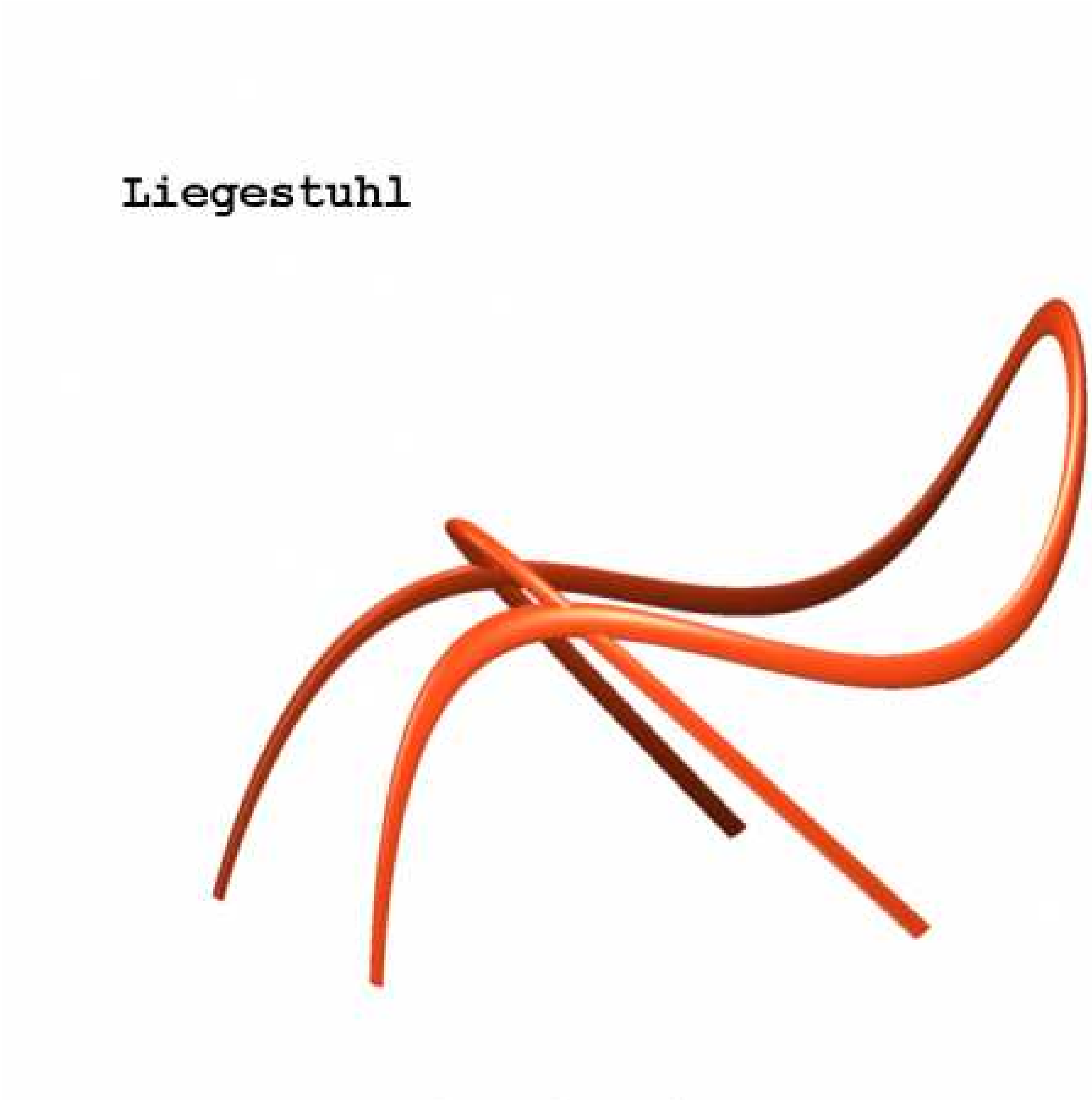
TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- Consider the equation

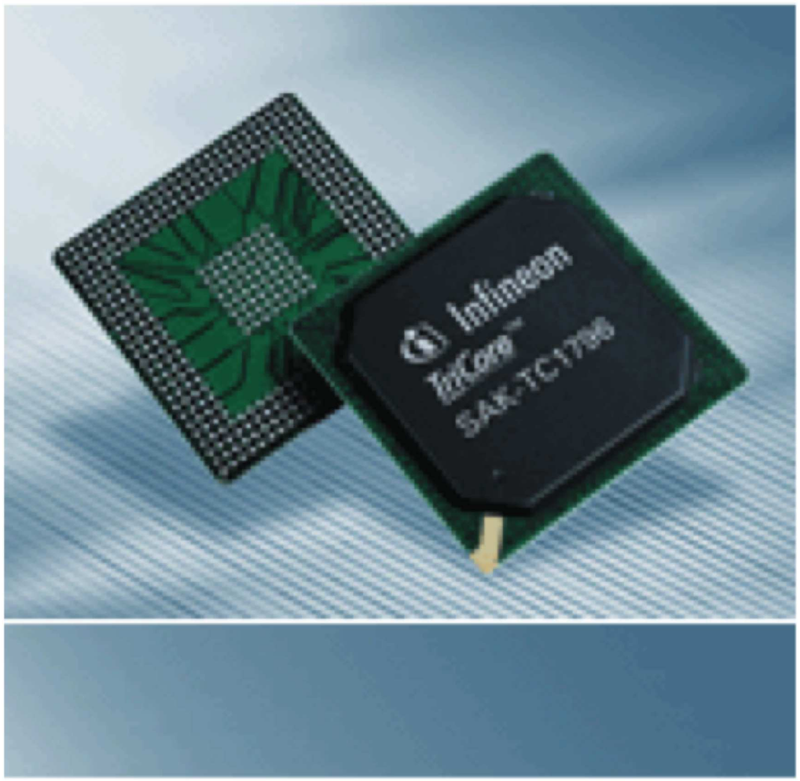
$$((y-z)^2+(y-1-\tfrac{1}{2}x-\tfrac{1}{8}x^2+\tfrac{1}{16}x^3)^2-\tfrac{1}{50})((x-\tfrac{3}{5}y+1)^2+(y-z^2)^2-\tfrac{1}{100})=0$$

- defining a surface of degree 10 in $\mathbb{R}^3$.
- What do you expect from the real picture?

Nice algebraic surfaces

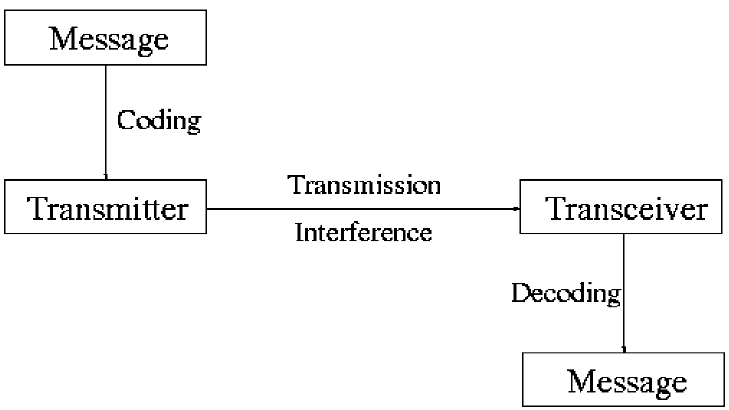


Infineon Tricore Project



- Aim: prove that the processor (32 Bit) works correctly
- every instruction of the processor will be verified specifying special properties and proving them
- it is difficult to check the arithmetic properties

Coding theorie



Coding theory: brnoeth.lib

- AG-Codes are codes, using algebraic vector spaces of divisors on algebraic curves over finite fields
- an implementation of the Brill-Noether algorithm for solving the Riemann-Roch problem and applications in Algebraic Geometry codes is implemented in SINGULAR.

Models for economy

Felix Kubler and Karl Schmedders (University of Zürich)

General problem:

- Study a computer model of a national economy,
  a standard exchange economy with finitely many agents and goods
- especially study equilibria
  Walrasian equilibrium consists of prices and choices, such that household maximize utilities, firms maximize profits and markets clear

Models for economy

Felix Kubler and Karl Schmedders (University of Zürich)

General problem:

- Study a computer model of a national economy,
  a standard exchange economy with finitely many agents and goods
- especially study equilibria
  Walrasian equilibrium consists of prices and choices, such that household maximize utilities, firms maximize profits and markets clear

Mathematical problem:
Find the positive real roots of a given system of polynomial equations

equilibrium model with production

```
ring R = 0,x(1..22),dp;
ideal I = -1+x(1)^5*x(4)*x(13),      -1+x(2)^5*x(4)*x(14),
-1+x(3)^5*x(4)*x(15),     -1+x(5)^3*x(8)*x(13),        -1+x(6)^3*x(8)*x(14),
-1+x(7)^3*x(8)*x(15),                              -1+x(9)^4*x(12)*x(13),
-1+x(10)^4*x(12)*x(14),                          -1+x(11)^4*x(12)*x(15),
5+2*x(16)-x(1)*x(13)-x(2)*x(14)-x(3)*x(15),
3+5*x(16)-x(5)*x(13)-x(6)*x(14)-x(7)*x(15),
(x(1)+x(5)+x(9))^3-x(17)^2*x(18),
(x(2)+x(6)+x(10))^2-x(19)*x(20),
(x(3)+x(7)+x(11))^2-4*x(21)*x(22),
x(17)+x(19)+x(21)-10,                              x(18)+x(20)+x(22)-10,
8*x(13)^3*x(18)-27*x(16)^3*x(17),    x(13)^3*x(17)^2-27*x(18)^2,
x(14)^2*x(20)-4*x(16)^2*x(19),          x(14)^2*x(19)-4*x(20),
x(15)^2*x(22)-x(16)^2*x(21),              x(15)^2*x(21)-x(22);
```

Sudoku

				5			8	
				6	2			5
6			4			7		
		7				9	6	
		5	2		6	1		
	3	6				4		
		3			7			4
1			5	8				
	6			1				

Sudoku

- the idea of a Sudoku goes back to Leonard Euler: Latin squares
- in our days invented by Howard Garns (USA): Number place

Sudoku

- the idea of a Sudoku goes back to Leonard Euler: Latin squares
- in our days invented by Howard Garns (USA): Number place
- associate to the places in a Sudoku the variables $x_1, \dots, x_{81}$ and to each variable x_i the polynomial $F_i(x_i) = \prod_{j=1}^{9}(x_i - j)$
- Let $E = \{(i,j), i < j$ and i,j in the same row, column or $3 \times 3 -$ box$\}$
- For $(i,j) \in E$ let $G_{i,j} = \frac{F_i - F_j}{x_i - x_j}$.
- Let $I \subset \mathbb{Q}[x_1, \dots, x_{81}]$ be the ideal generated by the 891 polynomials $\{G_{i,j}\}_{(i,j)\in E}$ and $\{F_i\}_{i=1,\dots,9}$
- $a = (a_1, \dots, a_{81}) \in V(I)$ iff $a_i \in \{1, \dots, 9\}$ and $a_i \neq a_j$ for $(i,j) \in E$

Sudoku

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- a well posed Sudoku has a unique solution.
- Let $L \subset \{1, \ldots, 81\}$ be the set of pre-assigned places and $\{a_i\}_{i \in L}$ the corresponding numbers of a concrete Sudoku S.
- Then $I_S = I + < \{x_i - a_i\}_{i \in L} >$ is the ideal associated to the Sudoku S.

Sudoku

- a well posed Sudoku has a unique solution.
- Let $L \subset \{1, \ldots, 81\}$ be the set of pre-assigned places and $\{a_i\}_{i \in L}$ the corresponding numbers of a concrete Sudoku S.
- Then $I_S = I + < \{x_i - a_i\}_{i \in L} >$ is the ideal associated to the Sudoku S.
- The reduced Gröbner basis of I_S with respect to the lexicographical ordering has the shape $x_1 - a_1, \ldots, x_{81} - a_{81}$ and $(a_1, \ldots, a_{81})$ is the solution of the Sudoku.

Computeralgebra and finite Groups

Problem: Characterize the class of finite solvable groups G by 2–variable identities.

Computeralgebra and finite Groups

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

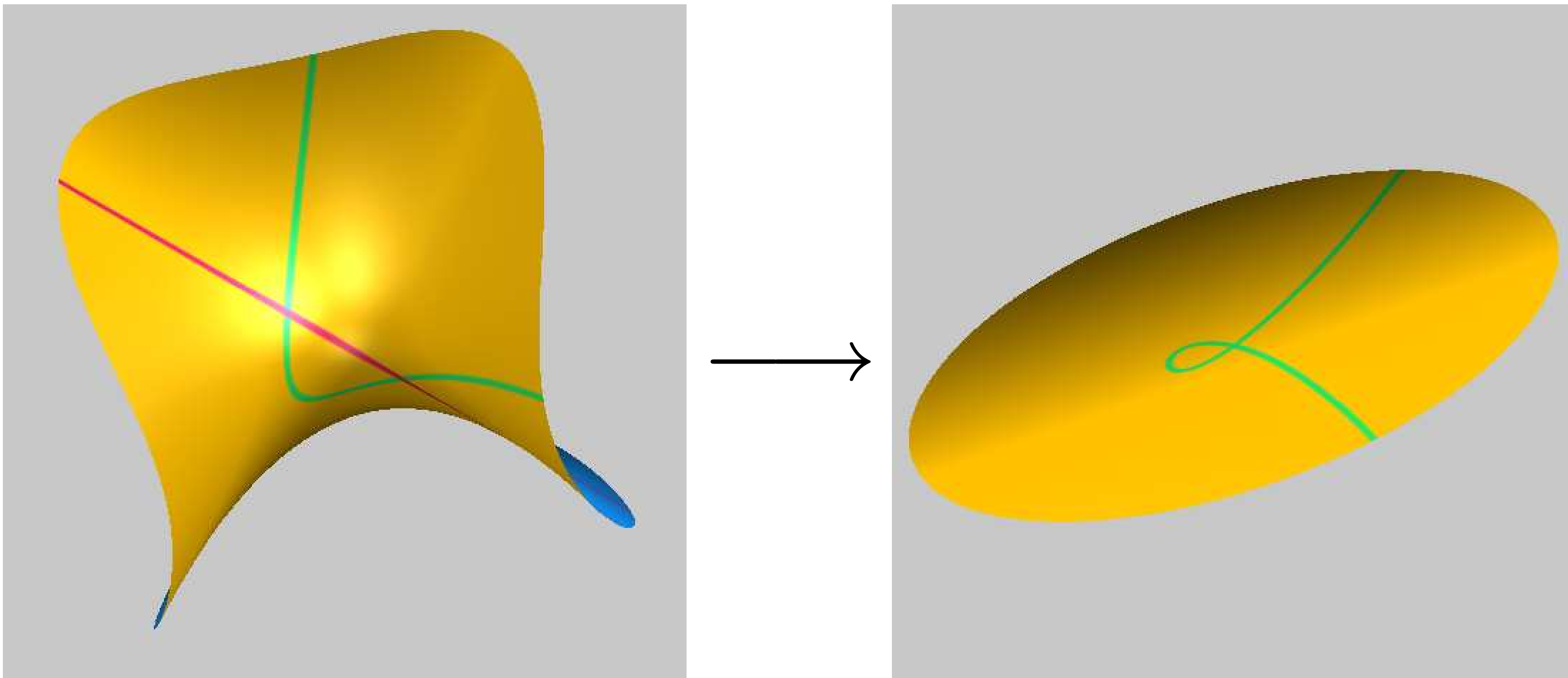
Problem: Characterize the class of finite solvable groups G by 2–variable identities.

Example:

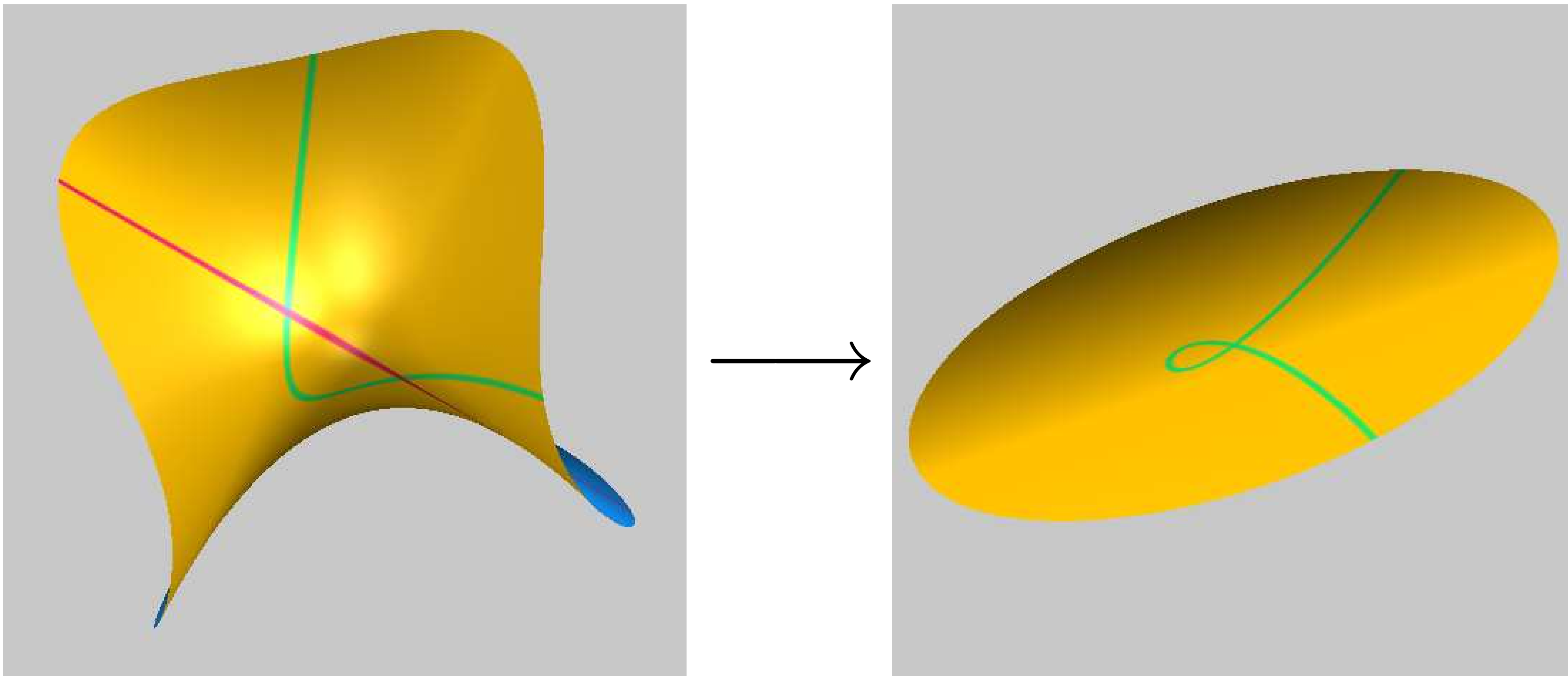
- G is **abelian** $\Leftrightarrow xy = yx \; \forall \; x, y \in G$
- (Zorn, 1930) A finite group G is **nilpotent** $\Leftrightarrow \exists \; n \geq 1$, such that $v_n(x, y) = 1 \; \forall \; x, y \in G$
  (**Engel Identity**)

  $v_1 := [x, y] = xyx^{-1}y^{-1}$ (commutator)
  $v_{n+1} := [v_n, y]$

Blowing up a node

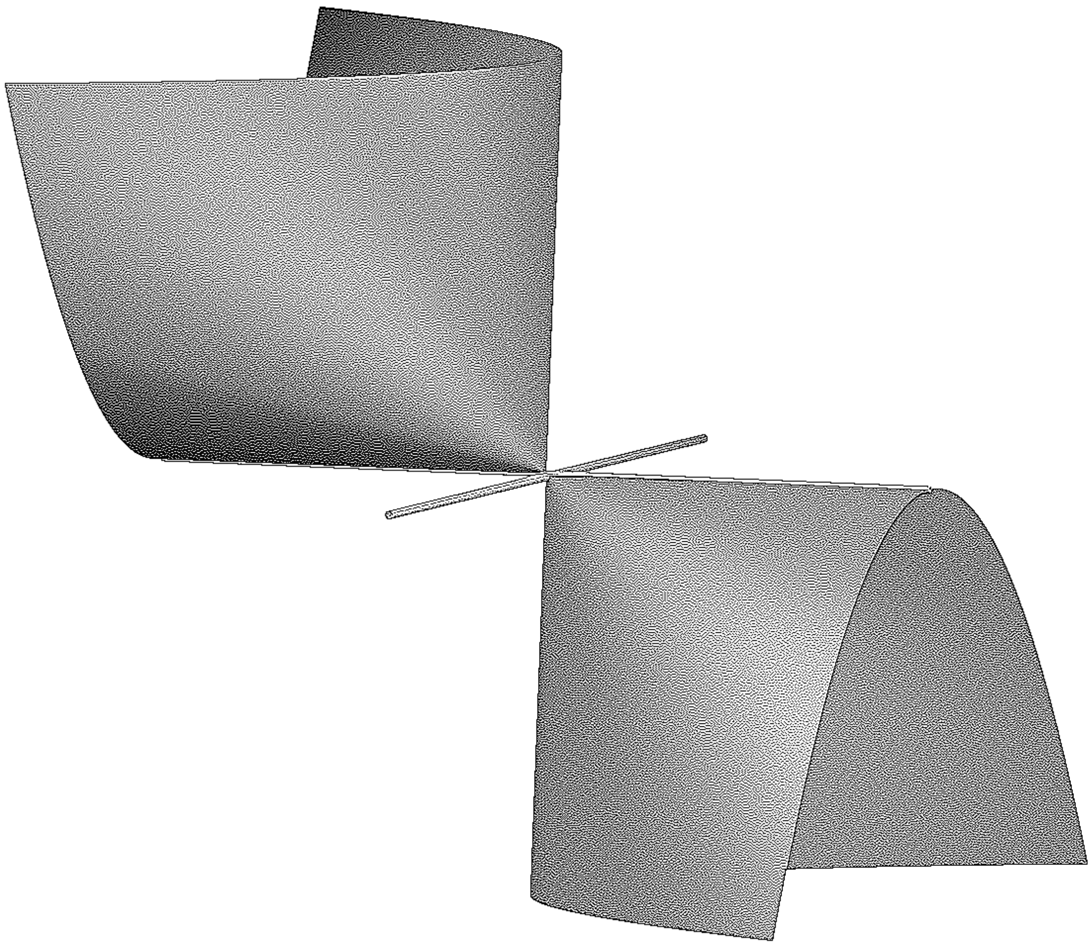


Blowing up a node

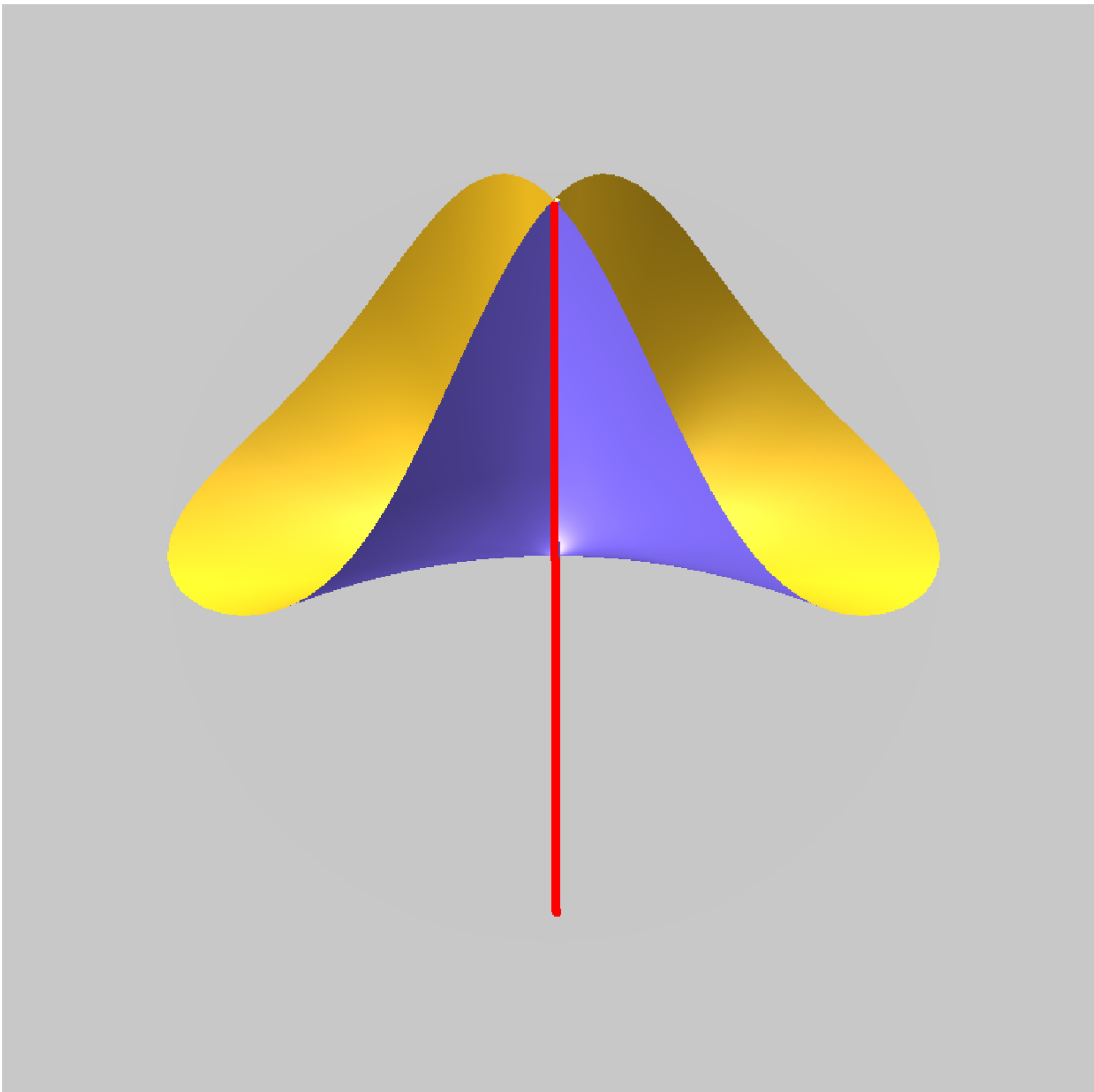


$$\pi : X = \{(x, y; u : v) \in K^2 \times \mathbb{P}^1 \mid xv = yu\} \longrightarrow K^2.$$

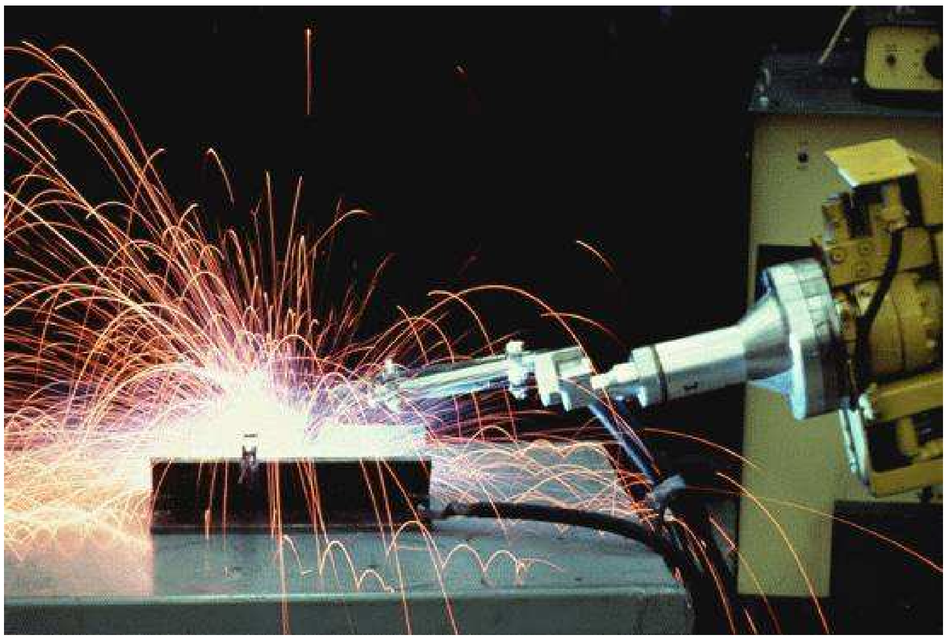
Primary decomposition



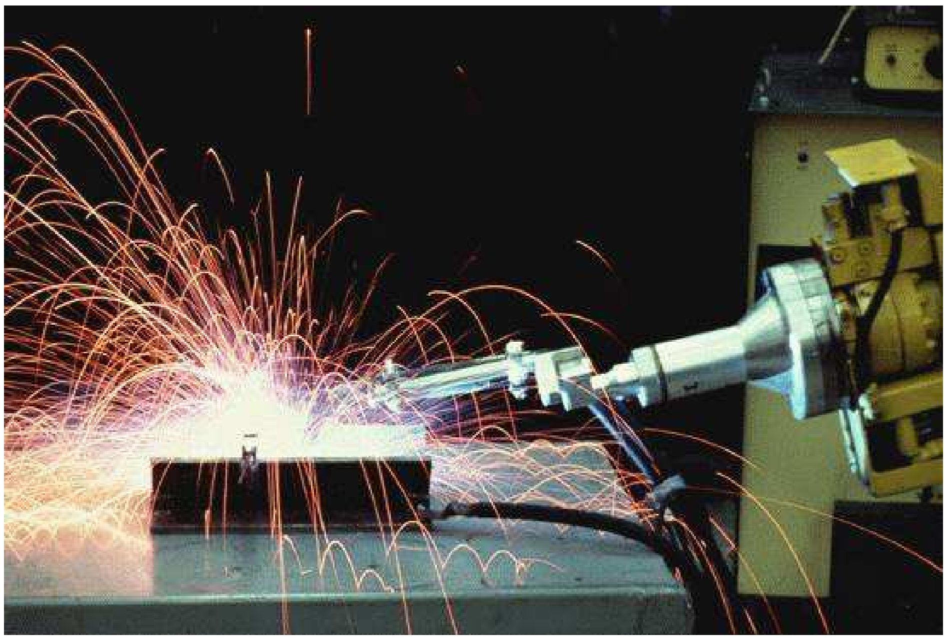
Primary decomposition



Robotics and the Cycloheptane Molecule

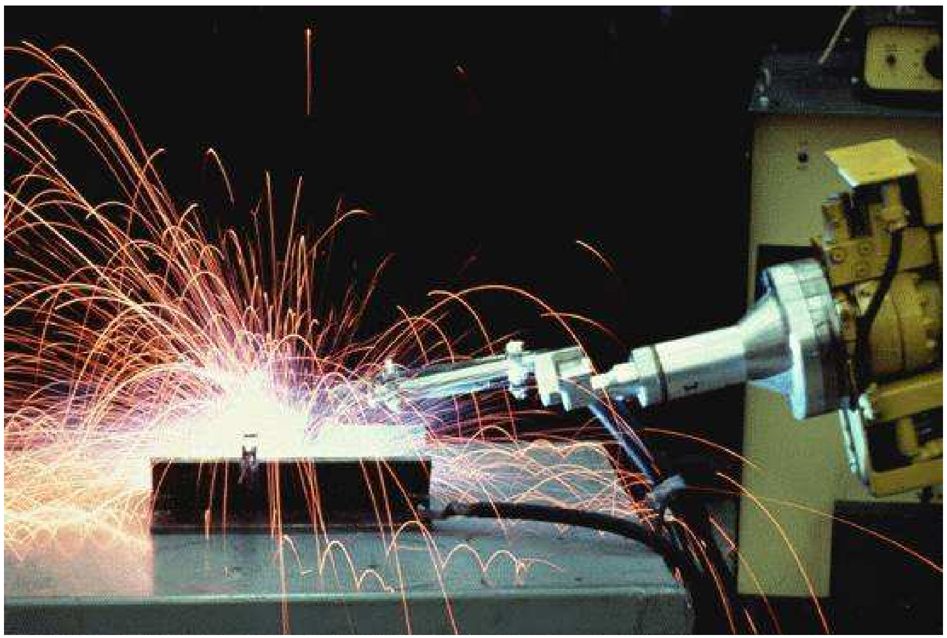


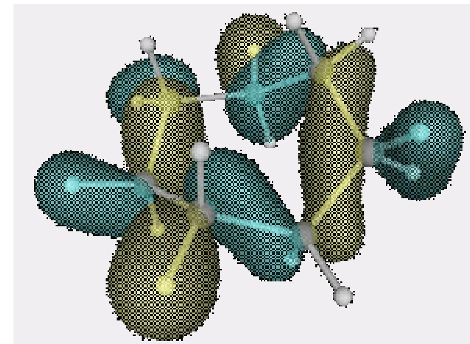
Robotics and the Cycloheptane Molecule

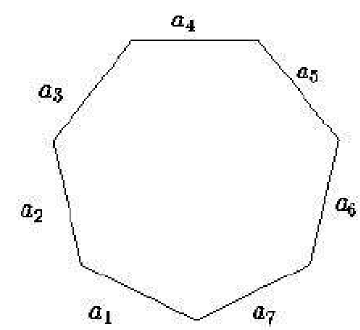


A.H.M. Levelt

Robotics and the Cycloheptane Molecule

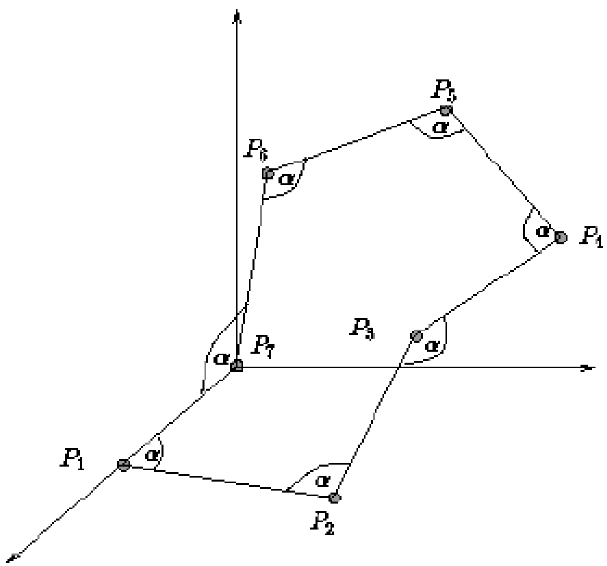




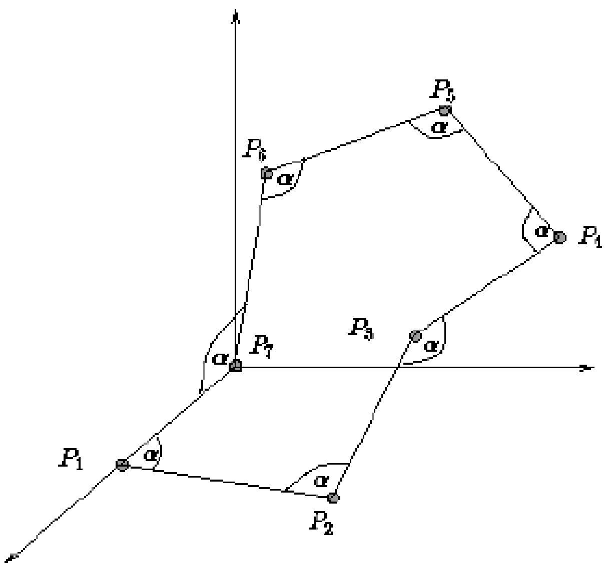


A.H.M. Levelt

The Heptagon



The Heptagon

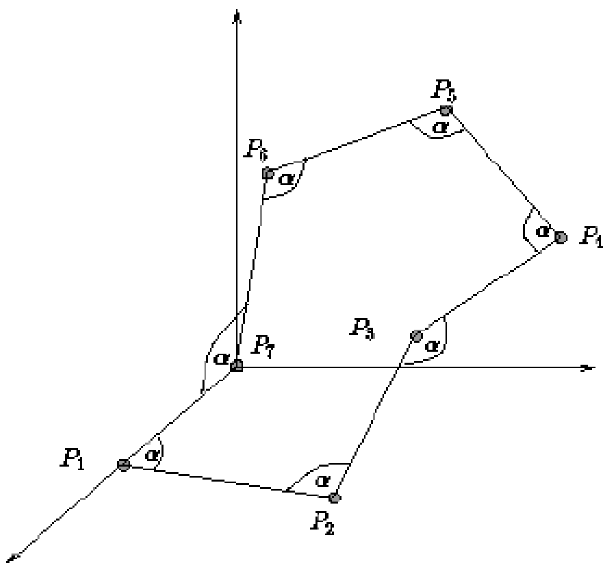


Equations for the vectors:

- $(a_1, a_2) = (a_2, a_3) = \ldots = (a_7, a_1) = c$
- $(a_1, a_1) = (a_2, a_2) = \ldots = (a_7, a_7) = 1$
- $a_1 + a_2 + \ldots + a_7 = 0$

$c = cos(\alpha)$ and $(,)$ is the scalar product.

The Heptagon



Equations for the vectors:

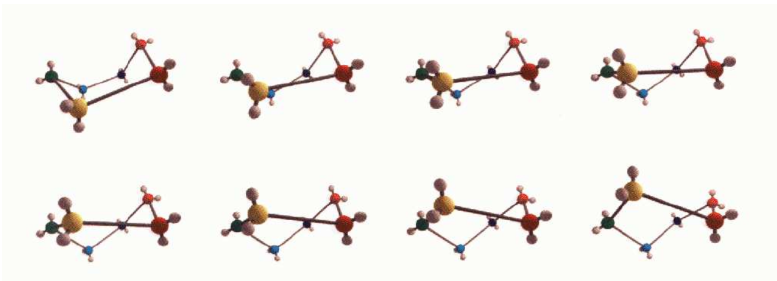
- $(a_1, a_2) = (a_2, a_3) = \ldots = (a_7, a_1) = c$
- $(a_1, a_1) = (a_2, a_2) = \ldots = (a_7, a_7) = 1$
- $a_1 + a_2 + \ldots + a_7 = 0$

$c = cos(\alpha)$ and $(,)$ is the scalar product.

- For $c = 0$: equations for the configuration space of a robot
- For $c = \frac{1}{3}$: equations for the configurations space of a molecule

The Molecule

Equations for the configuration space (in SINGULAR):



```
ring R=0,(v,w,x,y,z),dp;
ideal I=
81y2z2-54wyz+54y2z+54yz2-72w2+198wy-207y2+198wz-225yz-207z2+114w-141y-141z+10,
81w2x2+54w2x+54wx2-54wxz-207w2-225wx-207x2+198wz+198xz-72z2-141w-141x+114z+10,
324vw2x+432vw2+540vwx+432w2x-432wxy-432vwz+324wyz+180vw+846w2-576vx+180wx-
306wy+144xy+144vz-306wz-36yz+12v+585w+12x-318y-318z-79,
81v2w2+54v2w+54vw2-54vwy-207v2-225vw-207w2+198vy+198wy-72y2-141v-141w+114y+10;
```

The Projection

The equations describe a curve in $\mathbb{R}^5$. The projection to the w, x–plane is difficult to compute:

The Projection

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

The equations describe a curve in $\mathbb{R}^5$. The projection to the w, x–plane is difficult to compute:

13343098629642274643741505w20x16+18458805154059402163602552w20x15
+12528539096440613433050772w19x16-307469543636682571308498792w20x14
-308745089273555811810514188w19x15-335770469789305978523636514w18x16

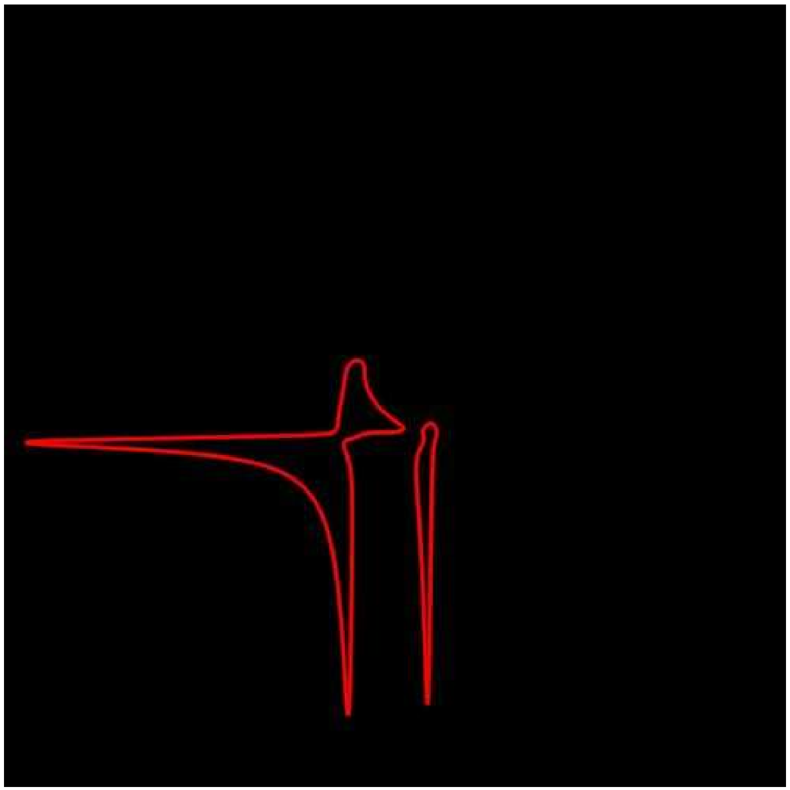
.

.

.

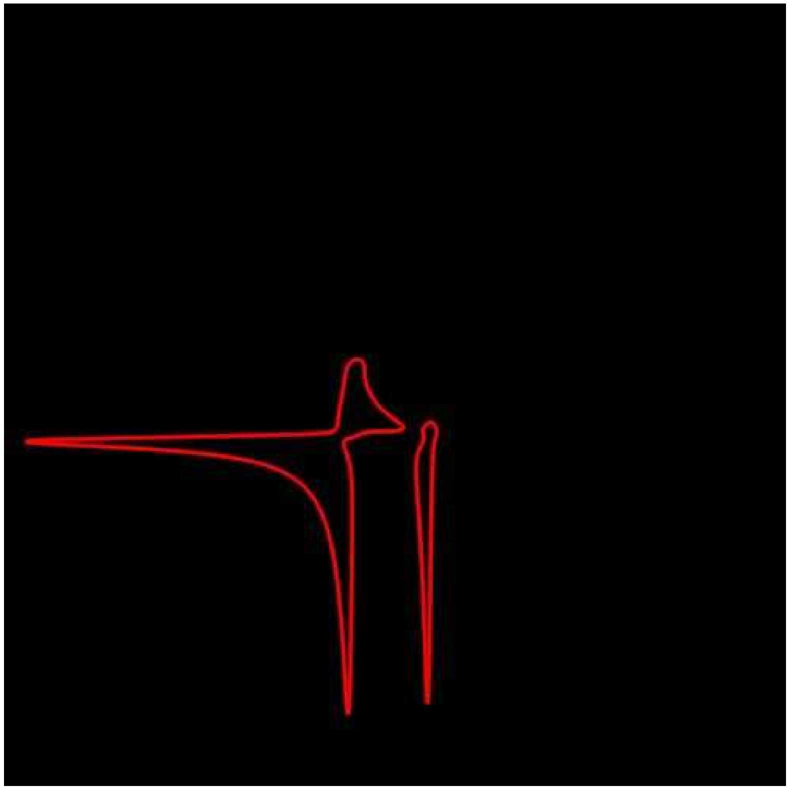
-57603722394732542788396875000w2x-56209703485755917382271875000wx2
-29459059311819369252628125000x3-3456386878638867977468750000w2
-388065077492910629437500000wx-3500955605594366547468750000x2
+1264097844032306972500000000w+1126578705265908772500000000x
+24065849284119685000000000

Projection of the curve to the w, x–plane



```
ideal K = eliminate(I,vyz);
LIB''surf.lib'';
plot(K[1]);
```

Projection of the curve to the w, x–plane



```
ideal K = eliminate(I,vyz);
LIB''surf.lib'';
plot(K[1]);
```

The curve shows the possible w, x–coordinates of the molecule.

Fields

- rational numbers $\mathbb{Q}$ (charakteristic 0)
- finite fields $\mathbb{Z}/p\mathbb{Z}(p <= 2147483629)$
- finite fields $\mathbb{F}_{p^n}(p^n < 2^{15})$

Fields

- rational numbers $\mathbb{Q}$ (charakteristic 0)
- finite fields $\mathbb{Z}/p\mathbb{Z}(p <= 2147483629)$
- finite fields $\mathbb{F}_{p^n}(p^n < 2^{15})$
- trancendental extensions of $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$
- algebraic extensions of $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$
  $K[t]$/MinPoly

Fields

- rational numbers $\mathbb{Q}$ (charakteristic 0)
- finite fields $\mathbb{Z}/p\mathbb{Z}(p <= 2147483629)$
- finite fields $\mathbb{F}_{p^n}(p^n < 2^{15})$
- trancendental extensions of $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$
- algebraic extensions of $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$
  $K[t]$/MinPoly
- floating point real and complex numbers

Rings

- polynomial rings $K[x_1, \ldots, x_n]$
- localizations $K[x_1, \ldots, x_n]_M$
  M maximal ideal
- factor rings $K[x_1, \ldots, x_n]/J$ oder $K[x_1, \ldots, x_n]_M/J$

Rings

- polynomial rings $K[x_1, \ldots, x_n]$
- localizations $K[x_1, \ldots, x_n]_M$
  M maximal ideal
- factor rings $K[x_1, \ldots, x_n]/J$ oder $K[x_1, \ldots, x_n]_M/J$
- non-commutative G–algebras
  $K\langle x_1, \ldots, x_n \mid x_j x_i = C_{ij} x_i x_j + D_{ij} \rangle$
  $C_{ij} \in K \;,\; LM(D_{ij}) < x_i x_j$
- factor algebras of G–algebras by two-sided ideals

Rings

- polynomial rings $K[x_1, \ldots, x_n]$
- localizations $K[x_1, \ldots, x_n]_M$
  M maximal ideal
- factor rings $K[x_1, \ldots, x_n]/J$ oder $K[x_1, \ldots, x_n]_M/J$
- non-commutative G–algebras
  $K\langle x_1, \ldots, x_n \mid x_j x_i = C_{ij} x_i x_j + D_{ij} \rangle$
  $C_{ij} \in K \;,\; LM(D_{ij}) < x_i x_j$
- factor algebras of G–algebras by two-sided ideals
- tensor products of the rings above

Algorithms in the Kernel (C/C_{++})

- Standard basis algorithms (Buchberger, SlimGB, factorizing Buchberger, FGLM, Hilbert–driven Buchberger, ...)

Algorithms in the Kernel (C/C_{++})

- Standard basis algorithms (Buchberger, SlimGB, factorizing Buchberger, FGLM, Hilbert–driven Buchberger, ...)
- Syzygies, free resolutions (Schreyer, La Scala, ...)

Algorithms in the Kernel (C/C_{++})

- Standard basis algorithms (Buchberger, SlimGB, factorizing Buchberger, FGLM, Hilbert–driven Buchberger, ...)
- Syzygies, free resolutions (Schreyer, La Scala, ...)
- Multivariate polynomial factorization
- absolute factorization (factorization over algebraically closed fields)

Algorithms in the Kernel (C/C_{++})

- Standard basis algorithms (Buchberger, SlimGB, factorizing Buchberger, FGLM, Hilbert–driven Buchberger, ...)
- Syzygies, free resolutions (Schreyer, La Scala, ...)
- Multivariate polynomial factorization
- absolute factorization (factorization over algebraically closed fields)
- Ideal theorie (intersection, quotient, elimination, saturation)

Algorithms in the Kernel (C/C_{++})

- Standard basis algorithms (Buchberger, SlimGB, factorizing Buchberger, FGLM, Hilbert–driven Buchberger, ...)
- Syzygies, free resolutions (Schreyer, La Scala, ...)
- Multivariate polynomial factorization
- absolute factorization (factorization over algebraically closed fields)
- Ideal theorie (intersection, quotient, elimination, saturation)
- combinatorics (dimension, Hilbert polynomial, multiplicity, ...)

Algorithms in the Kernel (C/C_{++})

- Standard basis algorithms (Buchberger, SlimGB, factorizing Buchberger, FGLM, Hilbert–driven Buchberger, ...)
- Syzygies, free resolutions (Schreyer, La Scala, ...)
- Multivariate polynomial factorization
- absolute factorization (factorization over algebraically closed fields)
- Ideal theorie (intersection, quotient, elimination, saturation)
- combinatorics (dimension, Hilbert polynomial, multiplicity, ...)
- many libraries: ... control.lib, surf.lib, solve.lib, primdec.lib, resolve.lib,....

Applications

- **mathematical**
  - experimental tool
  - proving theorems

Applications

- **mathematical**
  - experimental tool
  - proving theorems
- **non–mathematical**
  - engineering (glas melting, robotics, chemical models, analog and digital microelectronics)
  - equilibrian problems in economics
  - theoretical physics