Algebraic Geometry in Applications

Gerhard Pfister

TU Kaiserslautern

Lahore, August 2018

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

http://www.mathematik.uni-kl.de/ pfister/vortragLahore.pdf

Elimination

- lexikographical ordering

$x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} > x_1^{\beta_1} \cdot \ldots \cdot x_n^{\beta_n}$ if $\alpha_j = \beta_j$ for $j \leq k-1$ and $\alpha_k > \beta_k$

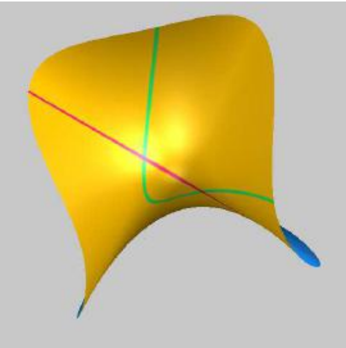
Elimination

- lexikographical ordering

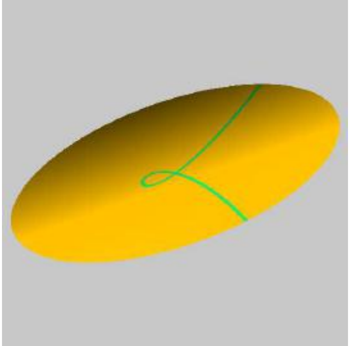
  $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} > x_1^{\beta_1} \cdot \ldots \cdot x_n^{\beta_n}$ if $\alpha_j = \beta_j$ for $j \leq k-1$ and $\alpha_k > \beta_k$

- $I \subset K[x_1, \ldots, x]$ ideal, G Gröbner basis, then $G \cap K[x_k, \ldots, x_n]$ is a Gröbner basis of $I \cap K[x_k, \ldots, x_n]$.
- this means geometrically to compute the projection $\pi : V(I) \subset K^n \longrightarrow K^{n-k+1}$.

Projection



$\longrightarrow$



$$\pi : V(z^2 - x + 1, y - xz) \subset \mathbb{C}^3 \longrightarrow V(x^3 - x^2 - y^2) \subset \mathbb{C}^2.$$

Infineon Tricore Project

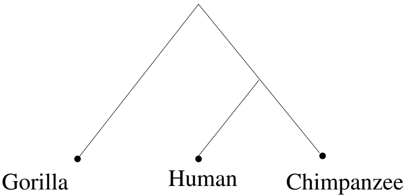
- Aim: prove that the processor (32 Bit) works correctly
- every instruction of the processor will be verified specifying special properties and proving them
- it is difficult to check the arithmetic properties

Robotics

Robotics

Computational Biology

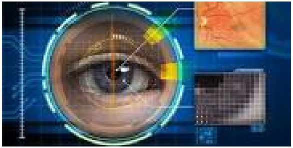
Phylogenetics is the study of the evolution of a set of species from a common ancestor. The evolution will be described using a **phylogenetic tree**.



To reconstruct such a tree pieces of DNA sequences are used.

Gorilla	AAGCTTCACCGGCGCAGTTGTTCTTATAATTGCCCACGGACTTACATCAT
Cimpanzee	AAGCTTCACCGGCGCAATTATCCTCATAATCGCCCACGGACTTACATCCT
Human	AAGCTTCACCGGCGCAGTCATTCTCATAATCGCCCACGGGCTTACATCCT

Computer Vision



The Perspective-n-Point problem, i.e. the problem of determining the absolute position and orientation of a camera given its intrinsic parameters and a set of n 2D-to-3D point correspondences, is one of the most important problems in computer vision with a broad range of applications in structure from motion or recognition.

Models for Economy

Felix Kubler and Karl Schmedders (University of Zürich)

General problem:

- Study a computer model of a national economy,

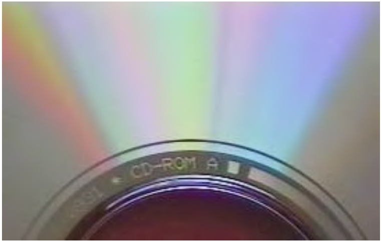
  a standard exchange economy with finitely many agents and goods

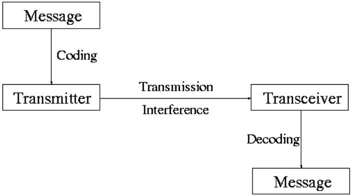
- especially study equilibria

  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

Coding theorie





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				

Abbildung: Sudoku

A Problem of Group Theory Solved Using Algebraic Gometry and Computer Algebra

Let G be a finite group, define

$$G^{(1)} := [G, G] = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle .$$

and $G^{(i)} := [G^{(i-1)}, G]$.
G is called nilpotent, if $G^{(m)} = \{e\}$ for some m.

Let G be a finite group, define

$$G^{(1)} := [G, G] = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle \, .$$

and $G^{(i)} := [G^{(i-1)}, G]$.
G is called nilpotent, if $G^{(m)} = \{e\}$ for some m.

- Abelian groups are nilpotent.
- If the order of G is a power of a prime, G is nilpotent.
- G is nilpotent $\Leftrightarrow$ it is a direct product of its Sylow groups.
- S_3 is not nilpotent.

Nilpotent Groups

Magma:

```
> G:=Sym(3);
> H:=CommutatorSubgroup(G,G);
H;
Permutation group acting on a set of cardinality 3
Order = 3
   (1, 2, 3)

> CommutatorSubgroup(H,G);
Permutation group acting on a set of cardinality 3
Order = 3
    (1, 2, 3)
```

Dihedral Group

$$D_4 =< r, s | r^4 = s^2 = e, srs = r^{-1} >$$

```
> #DihedralGroup(4);
8
> G:=CommutatorSubgroup(DihedralGroup(4),DihedralGroup(4));
Permutation group acting on a set of cardinality 4
Order = 2
   (1, 3)(2, 4)

> CommutatorSubgroup(G,DihedralGroup(4));
Permutation group acting on a set of cardinality 4
Order = 1
```

Solvable groups

Now define

$$G^{(i)} := [G^{(i-1)}, G^{(i-1)}],$$

then G is called solvable, if $G^{(m)} = \{e\}$ for a suitable m.

Solvable groups

Now define

$$G^{(i)} := [G^{(i-1)}, G^{(i-1)}],$$

then G is called solvable, if $G^{(m)} = \{e\}$ for a suitable m.

- nilpotente groups are solvable.
- S_3, S_4 are solvable.
- groups of odd order are solvable.
- S_5, A_5 are not solvable.

PSL

$$\mathrm{PSL}(2,K) = \ \mathrm{SL}(2,K)/\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \;\middle|\; a^2 = 1\right\}$$

PSL

$$\mathrm{PSL}(2,K) = \ \mathrm{SL}(2,K)/\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \;\middle|\; a^2 = 1\right\}$$

especially

$$\mathrm{PSL}(2,\mathbb{F}_5) = \{[\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)],\ a_{11}a_{22} - a_{21}a_{12} = 1\}$$
$$[\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)] = \left\{\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right),\ \begin{pmatrix} 4a_{11} & 4a_{12} \\ 4a_{21} & 4a_{22} \end{pmatrix}\right\}.$$

PSL

$$\mathrm{PSL}(2,K) = \mathrm{SL}(2,K)/\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \;\middle|\; a^2 = 1\right\}$$

especially

$$\mathrm{PSL}(2,\mathbb{F}_5) = \{[\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)],\ a_{11}a_{22} - a_{21}a_{12} = 1\}$$
$$[\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)] = \left\{\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right),\ \begin{pmatrix} 4a_{11} & 4a_{12} \\ 4a_{21} & 4a_{22} \end{pmatrix}\right\}.$$

It holds:

$$\mathrm{PSL}(2,\mathbb{F}_5) \cong \mathrm{PSL}(2,\mathbb{F}_4) \cong A_5$$

Solvable groups

```
> G:=PSL(2,5);

> G;

Permutation group G acting on a set of cardinality 6

Order = 60 = 2^2 * 3 * 5

    (3, 4)(5, 6)

    (1, 6, 2)(3, 4, 5)


> IsIsomorphic(G,Alt(5));

true Homomorphism of GrpPerm: G, Degree 6, Order 2^2 * 3 * 5 into

GrpPerm: $, Degree 5, Order 2^2 * 3 * 5 induced by

    (3, 4)(5, 6) |--> (1, 3)(2, 5)

    (1, 6, 2)(3, 4, 5) |--> (1, 4, 2)
```

Computeralgebra and finite Groups

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

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)
  $v_{n+1} := [v_n, y]$

Main Result

Theorem (T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavsky, G. Pfister, E. Plotkin)

$$U_1 = U_1(x,y) := x^{-2}y^{-1}x,$$
$$U_{n+1} = U_{n+1}(x,y) = [xU_nx^{-1}, yU_ny^{-1}].$$

A finite group G is **solvable** $\Leftrightarrow \exists\ n$, such that $U_n(x,y) = 1\ \forall\ x,y \in G$.

Main Result

Theorem (T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavsky, G. Pfister, E. Plotkin)

$$U_1 = U_1(x,y) := x^{-2}y^{-1}x,$$
$$U_{n+1} = U_{n+1}(x,y) = [xU_nx^{-1}, yU_ny^{-1}].$$

A finite group G is **solvable** $\Leftrightarrow \exists\ n$, such that $U_n(x,y) = 1\ \forall\ x,y \in G$.

- Let $x, y \in G$ such that $y \neq x^{-1}$ and $U_1(x,y) = U_2(x,y) \Rightarrow U_n(x,y) \neq 1\ \forall\ n \in \mathbb{N}$.

Proof

G solvable $\Rightarrow$ Identity is true (by definition).

Proof

G solvable $\Rightarrow$ Identity is true (by definition).

Idea of $\Leftarrow$

Theorem (Thompson, 1968) Let G be simple and minimally not solvable (i.e. G is not solvable but every proper subgroup is solvable). Then G is one of the following groups:

Proof

G solvable $\Rightarrow$ Identity is true (by definition).

Idea of $\Leftarrow$

Theorem (Thompson, 1968) Let G be simple and minimally not solvable (i.e. G is not solvable but every proper subgroup is solvable). Then G is one of the following groups:

- $\mathbf{PSL}(2, \mathbb{F}_p)$, p a prime number ≥ 5

Proof

G solvable $\Rightarrow$ Identity is true (by definition).

Idea of $\Leftarrow$

Theorem (Thompson, 1968) Let G be simple and minimally not solvable (i.e. G is not solvable but every proper subgroup is solvable). Then G is one of the following groups:

- $\mathbf{PSL}(2, \mathbb{F}_p)$, p a prime number ≥ 5
- $\mathbf{PSL}(2, \mathbb{F}_{2^p})$, p a prime number
- $\mathbf{PSL}(2, \mathbb{F}_{3^p})$, p a prime number

Proof

G solvable $\Rightarrow$ Identity is true (by definition).

Idea of $\Leftarrow$

Theorem (Thompson, 1968) Let G be simple and minimally not solvable (i.e. G is not solvable but every proper subgroup is solvable). Then G is one of the following groups:

- $\mathbf{PSL}(2, \mathbb{F}_p)$, p a prime number ≥ 5
- $\mathbf{PSL}(2, \mathbb{F}_{2^p})$, p a prime number
- $\mathbf{PSL}(2, \mathbb{F}_{3^p})$, p a prime number
- $\mathbf{PSL}(3, \mathbb{F}_3)$

Proof

G solvable $\Rightarrow$ Identity is true (by definition).

Idea of $\Leftarrow$

Theorem (Thompson, 1968) Let G be simple and minimally not solvable (i.e. G is not solvable but every proper subgroup is solvable). Then G is one of the following groups:

- $\mathbf{PSL}(2, \mathbb{F}_p)$, p a prime number ≥ 5
- $\mathbf{PSL}(2, \mathbb{F}_{2^p})$, p a prime number
- $\mathbf{PSL}(2, \mathbb{F}_{3^p})$, p a prime number
- $\mathbf{PSL}(3, \mathbb{F}_3)$
- $\mathbf{Sz}(2^p)$ p a prime number.

Proof

G solvable $\Rightarrow$ Identity is true (by definition).

Idea of $\Leftarrow$

Theorem (Thompson, 1968) Let G be simple and minimally not solvable (i.e. G is not solvable but every proper subgroup is solvable). Then G is one of the following groups:

- $\mathbf{PSL}(2, \mathbb{F}_p)$, p a prime number ≥ 5
- $\mathbf{PSL}(2, \mathbb{F}_{2^p})$, p a prime number
- $\mathbf{PSL}(2, \mathbb{F}_{3^p})$, p a prime number
- $\mathbf{PSL}(3, \mathbb{F}_3)$
- $\mathbf{Sz}(2^p)$ p a prime number.

If is enough to prove (for G in Thompson's list):

$\exists\, x, y \in G$, such that $y \neq x^{-1}$ and $U_1(x, y) = U_2(x, y)$.

Translation to algebraic Geometry

Let us consider $G = \mathbf{PSL}(2, \mathbb{F}_p), \ \mathbf{p} \geq \mathbf{5}$

Translation to algebraic Geometry

Let us consider $G = \mathbf{PSL}(2, \mathbb{F}_p),\ \mathbf{p} \geq \mathbf{5}$

Consider the matrices

$$x = \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix} \qquad y = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix}$$

$x^{-1} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & t \end{smallmatrix}\right)$ implies $y \neq x^{-1}$ for all $(b, c, t) \in \mathbb{F}_p^3$.

Translation to algebraic Geometry

Let us consider $G = \mathbf{PSL}(2, \mathbb{F}_p),\ \mathbf{p} \geq \mathbf{5}$

Consider the matrices

$$x = \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix} \qquad y = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix}$$

$x^{-1} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & t \end{smallmatrix}\right)$ implies $y \neq x^{-1}$ for all $(b, c, t) \in \mathbb{F}_p^3$.
It is enough to prove that the equation

$$U_1(x,y) = U_2(x,y), \text{ i.e.}$$
$$x^{-1}yx^{-1}y^{-1}x^2 = yx^{-2}y^{-1}xy^{-1}$$

has a solution $(b, c, t) \in \mathbb{F}_p^3$.

The equations

The entries of $U_1(x, y) - U_2(x, y)$ are the following polynomials $p_1, \ldots, p_4$ in $\mathbb{Z}[b, c, t]$. Let $I =< p_1, \ldots, p_4 >$.

$$
\begin{aligned}
p_1 = \quad & b^3c^2t^2 + b^2c^2t^3 - b^2c^2t^2 - bc^2t^3 - b^3ct + b^2c^2t + b^2ct^2 + 2bc^2t^2 \\
& + bct^3 + b^2c^2 + b^2ct + bc^2t - bct^2 - c^2t^2 - ct^3 - b^2t + bct + c^2t \\
& + ct^2 + 2bc + c^2 + bt +^2 ct + c + 1 \\
p_2 = \quad & -b^3ct^2 - b^2ct^3 + b^2c^2t + bc^2t^2 + b^3t - b^2ct - 2bct^2 - b^2c + bct \\
& + c^2t + ct^2 - bt - ct - b - c - 1 \\
p_3 = \quad & b^3c^3t^2 + b^2c^3t^3 - b^2c^2t^3 - bc^2t^4 - b^3c^2t + b^2c^3t +^2 b^2c^2t^2 \\
& + 2bc^3t^2 +^2 bc^2t^3 + b^2c^2t +^2 b^2ct^2 + bc^2t^2 - c^2t^3 - ct^4 - 2b^2ct \\
& + bc^2t + c^3t + bct^2 + 2c^2t^2 + ct^3 - b^2c - b^2t + bct + c^2t + bt^2 \\
& + 3ct^2 + bc - bt - b - c + 1 \\
p_4 = \quad & -b^3c^2t^2 - b^2c^2t^3 + b^2c^2t^2 + bc^2t^3 + b^3ct - b^2c^2t - b^2ct^2 - 2bc^2t^2 \\
& - bct^3 - 2b^2ct + c^2t^2 + ct^3 + b^2t - bct - c^2t - ct^2 + b^2 - bt \\
& - 2ct - b - t + 1
\end{aligned}
$$

The equations

The entries of $U_1(x,y) - U_2(x,y)$ are the following polynomials $p_1, \ldots, p_4$ in $\mathbb{Z}[b,c,t]$. Let $I =< p_1, \ldots, p_4 >$.

$$\begin{aligned}
p_1 = \quad & b^3c^2t^2 + b^2c^2t^3 - b^2c^2t^2 - bc^2t^3 - b^3ct + b^2c^2t + b^2ct^2 + 2bc^2t^2 \\
& + bct^3 + b^2c^2 + b^2ct + bc^2t - bct^2 - c^2t^2 - ct^3 - b^2t + bct + c^2t \\
& + ct^2 + 2bc + c^2 + bt +^2 ct + c + 1 \\
p_2 = \quad & -b^3ct^2 - b^2ct^3 + b^2c^2t + bc^2t^2 + b^3t - b^2ct - 2bct^2 - b^2c + bct \\
& + c^2t + ct^2 - bt - ct - b - c - 1 \\
p_3 = \quad & b^3c^3t^2 + b^2c^3t^3 - b^2c^2t^3 - bc^2t^4 - b^3c^2t + b^2c^3t +^2 b^2c^2t^2 \\
& + 2bc^3t^2 +^2 bc^2t^3 + b^2c^2t +^2 b^2ct^2 + bc^2t^2 - c^2t^3 - ct^4 - 2b^2ct \\
& + bc^2t + c^3t + bct^2 + 2c^2t^2 + ct^3 - b^2c - b^2t + bct + c^2t + bt^2 \\
& + 3ct^2 + bc - bt - b - c + 1 \\
p_4 = \quad & -b^3c^2t^2 - b^2c^2t^3 + b^2c^2t^2 + bc^2t^3 + b^3ct - b^2c^2t - b^2ct^2 - 2bc^2t^2 \\
& - bct^3 - 2b^2ct + c^2t^2 + ct^3 + b^2t - bct - c^2t - ct^2 + b^2 - bt \\
& - 2ct - b - t + 1
\end{aligned}$$

The zero set of I is a curve.

The equations

The entries of $U_1(x,y) - U_2(x,y)$ are the following polynomials $p_1, \ldots, p_4$ in $\mathbb{Z}[b,c,t]$. Let $I =< p_1, \ldots, p_4 >$.

$$
\begin{aligned}
p_1 = \quad & b^3c^2t^2 + b^2c^2t^3 - b^2c^2t^2 - bc^2t^3 - b^3ct + b^2c^2t + b^2ct^2 + 2bc^2t^2 \\
& + bct^3 + b^2c^2 + b^2ct + bc^2t - bct^2 - c^2t^2 - ct^3 - b^2t + bct + c^2t \\
& + ct^2 + 2bc + c^2 + bt +^2 ct + c + 1 \\
p_2 = \quad & -b^3ct^2 - b^2ct^3 + b^2c^2t + bc^2t^2 + b^3t - b^2ct - 2bct^2 - b^2c + bct \\
& + c^2t + ct^2 - bt - ct - b - c - 1 \\
p_3 = \quad & b^3c^3t^2 + b^2c^3t^3 - b^2c^2t^3 - bc^2t^4 - b^3c^2t + b^2c^3t +^2 b^2c^2t^2 \\
& + 2bc^3t^2 +^2 bc^2t^3 + b^2c^2t +^2 b^2ct^2 + bc^2t^2 - c^2t^3 - ct^4 - 2b^2ct \\
& + bc^2t + c^3t + bct^2 + 2c^2t^2 + ct^3 - b^2c - b^2t + bct + c^2t + bt^2 \\
& + 3ct^2 + bc - bt - b - c + 1 \\
p_4 = \quad & -b^3c^2t^2 - b^2c^2t^3 + b^2c^2t^2 + bc^2t^3 + b^3ct - b^2c^2t - b^2ct^2 - 2bc^2t^2 \\
& - bct^3 - 2b^2ct + c^2t^2 + ct^3 + b^2t - bct - c^2t - ct^2 + b^2 - bt \\
& - 2ct - b - t + 1
\end{aligned}
$$

The zero set of I is a curve.

We have to prove that for every prime p there are $\mathbb{F}_p$-rational points on the curve.

Hasse–Weil–Theorem

Theorem von Hasse–Weil (generalized by Aubry and Perret for singulare curves):

Hasse–Weil–Theorem

Theorem von Hasse–Weil (generalized by Aubry and Perret for singulare curves):
Let $C \subseteq \mathbb{A}^n$ be an absolutely irreducible affine curve defined over the finite field $\mathbb{F}_q$ and $\overline{C} \subset \mathbb{P}^n$ its projective closure $\Rightarrow$

$$\#C(\mathbb{F}_q) \geq q + 1 - 2p_a\sqrt{q} - d$$

($d =$ degree, $p_a =$ arithmetic genus of $\overline{C}$).

Hasse–Weil–Theorem

Theorem von Hasse–Weil (generalized by Aubry and Perret for singulare curves):
Let $C \subseteq \mathbb{A}^n$ be an absolutely irreducible affine curve defined over the finite field $\mathbb{F}_q$ and $\overline{C} \subset \mathbb{P}^n$ its projective closure $\Rightarrow$

$$\#C(\mathbb{F}_q) \geq q + 1 - 2p_a\sqrt{q} - d$$

($d =$ degree, $p_a =$ arithmetic genus of $\overline{C}$).

The Hilbert–polynomial of $\overline{C}$, $H(t) = d \cdot t - p_a + 1$, can be computed using the ideal I_h of $\overline{C}$:
We obtain $H(t) = 10t - 11 \Rightarrow d = 10,\ p_a = 12$.

Hasse–Weil–Theorem

Theorem von Hasse–Weil (generalized by Aubry and Perret for singulare curves):
Let $C \subseteq \mathbb{A}^n$ be an absolutely irreducible affine curve defined over the finite field $\mathbb{F}_q$ and $\overline{C} \subset \mathbb{P}^n$ its projective closure $\Rightarrow$

$$\#C(\mathbb{F}_q) \geq q + 1 - 2p_a\sqrt{q} - d$$

($d =$ degree, $p_a =$ arithmetic genus of $\overline{C}$).

The Hilbert–polynomial of $\overline{C}$, $H(t) = d \cdot t - p_a + 1$, can be computed using the ideal I_h of $\overline{C}$:
We obtain $H(t) = 10t - 11 \Rightarrow d = 10,\ p_a = 12$.
Since $p + 1 - 24\sqrt{p} - 10 > 0$ if $p > 593$, we obtain the result.

absolute irreduciblity

Proposition: $V(I^{(p)})$ is absolutely irreducibel for all primes $p \geq 5$.

absolute irreduciblity

Proposition: $V(I^{(p)})$ is absolutely irreducibel for all primes $p \geq 5$.
proof:

Using **SINGULAR** we show:

$$\langle f_1, f_2 \rangle : h^2 = I.$$

Proposition: $V(I^{(p)})$ is absolutely irreducibel for all primes $p \geq 5$.
proof:

Using **SINGULAR** we show:

$$\langle f_1, f_2 \rangle : h^2 = I.$$

$$\begin{aligned}
f_1 = \quad & t^2 b^4 + (t^4 - 2t^3 - 2t^2)b^3 - (t^5 - 2t^4 - t^2 - 2t - 1)b^2 \\
& -(t^5 - 4t^4 + t^3 + 6t^2 + 2t)b + (t^4 - 4t^3 + 2t^2 + 4t + 1) \\
f_2 = \quad & (t^3 - 2t^2 - t)c + t^2 b^3 + (t^4 - 2t^3 - 2t^2)b^2 \\
& -(t^5 - 2t^4 - t^2 - 2t - 1)b - (t^5 - 4t^4 + t^3 + 6t^2 + 2t) \\
h = \quad & t^3 - 2t^2 - t
\end{aligned}$$

absolute irreduciblity

Let $P(x) := t^2 J[1]|_{b=x/t}$ then P is monic of degree 4.

absolute irreduciblity

Let $P(x) := t^2 J[1]|_{b=x/t}$ then P is monic of degree 4.

$$x^4 + (t^3 - 2t^2 - 2t)x^3 - (t^5 - 2t^4 - t^2 - 2t - 1)x^2 - (t^6 - 4t^5 + t^4 + 6t^3 + 2t^2)x + (t^6 - 4t^5 + 2t^4 + 4t^3 + t^2).$$

We prove, that the induced polynomial $P \in \mathbb{F}_p[t, x]$ is absolutely irreducibel for all primes $p \geq 2$.
(Using the lemma of Gauß this is equivalent to P being irreducibel in $\overline{\mathbb{F}}_p(t)[x]$.)

absolute irreduciblity

Ansatz

$$(*) \quad P = (x^2 + ax + b)(x^2 + gx + d)$$

a, b, g, d polynomials in t with variable coefficients

$$a(i),\ b(i),\ g(i),\ d(i)\,.$$

absolute irreducibliity

Ansatz

$$(*) \quad P = (x^2 + ax + b)(x^2 + gx + d)$$

a, b, g, d polynomials in t with variable coefficients

$$a(i),\ b(i),\ g(i),\ d(i)\,.$$

The decomposition $(*)$ with `a(i)`, `b(i)`, `g(i)`, `d(i)` $\in \overline{\mathbb{F}}_p$ does not exist iff the ideal `C` generated by the coefficients with respect to x, t of $P - (x^2 + ax + b)(x^2 + gx + d)$ has no solution in $\overline{\mathbb{F}}_p$. This is equivalent to the fact that $1 \in$ `C`.

The ideal of the coefficients of C:

```
C[1]=-b(5)*d(3)
C[2]=-b(5)*g(2)
C[3]=-b(4)*d(3)-b(5)*d(2)
C[4]=-b(4)*g(2)-b(5)*g(1)-d(3)-1
C[5]=-b(3)*d(3)-b(4)*d(2)-b(5)*d(1)+1
C[6]=-b(5)-g(2)-1
C[7]=a(0)*b(5)-a(2)*d(3)-b(3)*g(2)-b(4)*g(1)-d(2)+4
C[8]=-a(0)^2*b(5)+b(0)*b(5)-b(2)*d(3)-b(3)*d(2)-b(4)*d(1)-b(5)-4
C[9]=-a(2)*g(2)-b(4)-g(1)+2
C[10]=a(0)*b(4)-a(1)*d(3)-a(2)*d(2)-b(2)*g(2)-b(3)*g(1)-d(1)-1
C[11]=-a(0)^2*b(4)+b(0)*b(4)-b(1)*d(3)-b(2)*d(2)-b(3)*d(1)-b(4)+2
C[12]=a(0)-a(1)*g(2)-a(2)*g(1)-b(3)-d(3)
C[13]=-a(0)^2+a(0)*b(3)-a(0)*d(3)-a(1)*d(2)-a(2)*d(1)+b(0)-b(1)*g(2)-b(2)*g(1)-7
C[14]=-a(0)^2*b(3)+b(0)*b(3)-b(0)*d(3)-b(1)*d(2)-b(2)*d(1)-b(3)+4
C[15]=-a(2)-g(2)-2
C[16]=a(0)*a(2)-a(0)*g(2)-a(1)*g(1)-b(2)-d(2)+1
C[17]=-a(0)^2*a(2)+a(0)*b(2)-a(0)*d(2)-a(1)*d(1)+a(2)*b(0)-a(2)-b(0)*g(2)-b(1)*g(1)-2
C[18]=-a(0)^2*b(2)+b(0)*b(2)-b(0)*d(2)-b(1)*d(1)-b(2)+1
C[19]=-a(1)-g(1)-2
C[20]=a(0)*a(1)-a(0)*g(1)-b(1)-d(1)+2
C[21]=-a(0)^2*a(1)+a(0)*b(1)-a(0)*d(1)+a(1)*b(0)-a(1)-b(0)*g(1)
C[22]=-a(0)^2*b(1)+b(0)*b(1)-b(0)*d(1)-b(1)
C[23]=-a(0)^3+2*a(0)*b(0)-a(0)
C[24]=-a(0)^2*b(0)+b(0)^2-b(0)
```

absolute irreduciblity

Using SINGULAR, one shows that over

$$\mathbb{Z}\big[\{a(i)\},\ \{b(i)\},\ \{g(i)\},\ \{d(i)\}\big]$$

$$4 = \sum_{i=1}^{24} M_i \ \mathtt{C}[i]\,.$$

Algebraic Statistics: Point of View of Algebraic Geometry

A statistical model in algebraic statistics is a polynomial map

$$\varphi : \mathbb{R}^d \to \mathbb{R}^m$$

Example

If X is the random variable [1] describing the number of heads in m flips of a coin, and $t \in [0,1]$ is the probability that we obtain head in one flip, then we can use the **binomial distribution** to model this situation:

$$\mathrm{Prob}(X = j) = \binom{m}{j} t^j (1-t)^{m-j} \ .$$

[1] A random variable is defined as a function that maps the outcomes of unpredictable processes to numerical quantities, typically real numbers.

Statistical Models

Example

If X is the random variable [1] describing the number of heads in m flips of a coin, and $t \in [0,1]$ is the probability that we obtain head in one flip, then we can use the **binomial distribution** to model this situation:

$$\operatorname{Prob}(X = j) = \binom{m}{j} t^j (1-t)^{m-j} \ .$$

These polynomials describe a map

$$\varphi : \mathbb{R} \to \mathbb{R}^{m+1}, t \mapsto (\ldots, \tbinom{m}{j} t^j (1-t)^{m-j}, \ldots).$$

[1] A random variable is defined as a function that maps the outcomes of unpredictable processes to numerical quantities, typically real numbers.

Statistical Models

Example

If X is the random variable [1] describing the number of heads in m flips of a coin, and $t \in [0,1]$ is the probability that we obtain head in one flip, then we can use the **binomial distribution** to model this situation:

$$\mathrm{Prob}(X = j) = \binom{m}{j} t^j (1-t)^{m-j} \ .$$

These polynomials describe a map

$$\varphi : \mathbb{R} \to \mathbb{R}^{m+1}, t \mapsto (\ldots, \tbinom{m}{j} t^j (1-t)^{m-j}, \ldots).$$

This map is our **statistical model**.

[1] A random variable is defined as a function that maps the outcomes of unpredictable processes to numerical quantities, typically real numbers.

Statistical Models

Example

If we regard φ as a map over the complex numbers

$$\varphi : \mathbb{C} \to \mathbb{C}^{m+1}, t \mapsto (\ldots, \tbinom{m}{j} t^j (1-t)^{m-j}, \ldots),$$

write $p_0, \ldots, p_m$ for the coordinate functions on $\mathbb{C}^{m+1}$, and consider the ideal

$$J := \langle \{p_j - \binom{m}{j} t^j (1-t)^{m-j}\}_{j=0,\ldots,m} \rangle \subseteq \mathbb{C}[p_0, \ldots, p_m, t],$$

then the elimination ideal $I = J \cap \mathbb{C}[p_0, \ldots, p_m]$ describes the Zariski closure of the image of φ.

Statistical Models

Example

If we regard φ as a map over the complex numbers

$$\varphi : \mathbb{C} \to \mathbb{C}^{m+1}, t \mapsto (\ldots, \tbinom{m}{j} t^j (1-t)^{m-j}, \ldots),$$

write $p_0, \ldots, p_m$ for the coordinate functions on $\mathbb{C}^{m+1}$, and consider the ideal

$$J := \langle \{p_j - \binom{m}{j} t^j (1-t)^{m-j}\}_{j=0,\ldots,m} \rangle \subseteq \mathbb{C}[p_0, \ldots, p_m, t],$$

then the elimination ideal $I = J \cap \mathbb{C}[p_0, \ldots, p_m]$ describes the Zariski closure of the image of φ. Every polynomial in I is called a **model invariant**.

Statistical Models

Based on observations in an experiment, we can use the model invariants to value t. We consider the case $m = 6$:

Example

```
ring R = 0, (p(0..6),t), dp;
ideal J = p(0)-(1-t)^6,p(1)-6t*(1-t)^5,
          p(2)-15t2*(1-t)^4,p(3)-20t3*(1-t)^3,
          p(4)-15t4*(1-t)^2,p(5)-6t5*(1-t),
          p(6)-t6;
ideal I = eliminate(J,t);
ring S = 0, p(0..6), dp;
ideal I = imap(R,I);
I;
```

Statistical Models

Example

```
I[1] =p(0)+p(1)+p(2)+p(3)+p(4)+p(5)+p(6)-1
I[2] =5*p(5)^2-12*p(4)*p(6)

...

I[16]=5*p(1)^2+7560*p(1)*p(6)+12600*p(2)*p(6)
      +16200*p(3)*p(6)+18900*p(4)*p(6)+21000*p(5)*p(6)
      +22680*p(6)^2-12*p(2)+54*p(3)-252*p(4)+1680*p(5)
      -22680*p(6)
```

Statistical Models

Example

Now suppose that we observed in an experiment that $p_3 = \frac{1}{4}$.
Then this determines the other p_i in the model.

```
LIB "solve.lib";
I = I, p(3)-1/4;
solve(I);
```

We obtain 6 solutions, 2 of which are real:

Statistical Models

Example

```
[1]:                  [2]:
   [1]:                  [1]:
      0.064862202           0.0024089531
   [2]:                  [2]:
      0.22479279            0.025023044
   [3]:                  [3]:
      0.32460995            0.10830306
   [4]:                  [4]:
      0.25                  0.25
   [5]:                  [5]:
      0.10830306            0.32460995
   [6]:                  [6]:
      0.025023044           0.22479279
   [7]:                  [7]:
      0.0024089531          0.064862202
```

Statistical Models

Example

From this we deduce that t is either 0.36613231 or 0.63386769. This shows that the coin is not fair (that is, the probability for head is different from $\frac{1}{2}$).

Algebraic Statistics

For the general situation let X be a discrete random [2] variable taking values in $\{1,\ldots,n\}$. Let the probabilities $P(X=i)$ be given parametrically by polynomials $p_i(t_1,\ldots,t_d)$. The statistical model in algebraic statistics is the polynomial map

$$\varphi:\mathbb{R}^d\to\mathbb{R}^n \ ,\varphi(t)=(p_1(t),\ldots,p_n(t)).$$

Consider in $\mathbb{C}[p_1,\ldots,p_n,t_1,\ldots,t_d]$ the ideal J generated by $\{p_i-p_i(t)\}_{i=1,\ldots,n}$. Over the complex numbers the elimination ideal $I=J\cap\mathbb{C}[p_1,\ldots,p_n]$ describes the Zariski closure of the image of φ, the model variety. Every polynomial in I is called a **model invariant**.

[2] A random variable is defined as a function that maps the outcomes of unpredictable processes to numerical quantities, typically real numbers.

Computational Biology

What is DNA =Deoxyribo Nucleic Acid?

- DNA molecules contain the biological instructions that make each species unique.

Computational Biology

What is DNA =Deoxyribo Nucleic Acid?

- DNA molecules contain the biological instructions that make each species unique.
- DNA is made of chemical building blocks called nucleotides. These building blocks are made of three parts: a phosphate group, a sugar group and one of four types of nitrogen bases. To form a strand of DNA, nucleotides are linked into chains.

Computational Biology

What is DNA =Deoxyribo Nucleic Acid?

- DNA molecules contain the biological instructions that make each species unique.
- DNA is made of chemical building blocks called nucleotides. These building blocks are made of three parts: a phosphate group, a sugar group and one of four types of nitrogen bases. To form a strand of DNA, nucleotides are linked into chains.
- The four types of nitrogen bases found in nucleotides are: adenine (A), thymine (T), guanine (G) and cytosine (C). The order, or sequence, of these bases determines what biological instructions are contained in a strand of DNA.

What is DNA =Deoxyribo Nucleic Acid?

- DNA molecules contain the biological instructions that make each species unique.
- DNA is made of chemical building blocks called nucleotides. These building blocks are made of three parts: a phosphate group, a sugar group and one of four types of nitrogen bases. To form a strand of DNA, nucleotides are linked into chains.
- The four types of nitrogen bases found in nucleotides are: adenine (A), thymine (T), guanine (G) and cytosine (C). The order, or sequence, of these bases determines what biological instructions are contained in a strand of DNA.
- DNA contains the instructions needed for an organism to develop, survive and reproduce.

Evolution and Mutations

Evolution depends on **mutations**, that is, changes in the nucleotide sequence of an organisms genetic material.

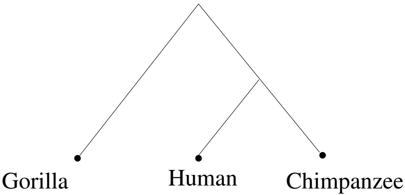
Phylogenetic Trees and Evolution

Given (parts of) the DNA of a number of living species, the goal in using phylogenetic trees is to obtain information on the least common ancestor. The living species are represented by the leaves of the tree, while the root will represent the least common ancestor of all considered species. We make the assumption, that the living species are represented by parts of DNA of equal lenghts:

```
Gorilla     AAGCTTCACCGGCGCAGTTGTTCTTATAATTGCCCACGGACTTACATCAT
Cimpanzee   AAGCTTCACCGGCGCAATTATCCTCATAATCGCCCACGGACTTACATCCT
Human       AAGCTTCACCGGCGCAGTCATTCTCATAATCGCCCACGGGCTTACATCCT
```

These are strings in the letters A, C, G, T representing the nucleotides.

Phylogenetic Tree



This tree has 5 nodes including the three leaves corresponding to Gorilla, Human, Chimpanzee.
The node on top of the tree is called root (common ancestor).

Phylogenetic Trees and Evolution

We assume that only substitutions occur during the evolutionary process and that this satisfies the following conditions:

(1) Each nucleotide of the sequence evolves independently of the other nucleotides and in the same way (identically distributed).

(2) The state at a node only depends on the previous state.[3]

(3) At bifurcating branches the process is independent on the common node.

[3] A process with this property is called a **Markov Process**.

Phylogenetic Trees and Evolution

We consider a so-called phylogenetic tree $\mathcal{T}$ to model the situation: We think of the edges of the tree as evolutionary steps.

Phylogenetic Trees and Evolution

We consider a so-called phylogenetic tree $\mathcal{T}$ to model the situation: We think of the edges of the tree as evolutionary steps.
For a node v, we denote by P_X^v the probability having $X \in \{A, C, G, T\}$ at a certain position of the DNA string at this node, and write $P^v = (P_A^v, P_C^v, P_G^v, P_T^v)$.

Phylogenetic Trees and Evolution

We consider a so-called phylogenetic tree $\mathcal{T}$ to model the situation: We think of the edges of the tree as evolutionary steps.
For a node v, we denote by P_X^v the probability having $X \in \{A, C, G, T\}$ at a certain position of the DNA string at this node, and write $P^v = (P_A^v, P_C^v, P_G^v, P_T^v)$.
To each edge $e = (v_1, v_2)$ we associate a matrix of probabilities

$$M_e = \begin{pmatrix} P_{A|A} & \cdots & P_{T|A} \\ P_{A|C} & \cdots & P_{T|C} \\ P_{A|G} & \cdots & P_{T|G} \\ P_{A|T} & \cdots & P_{T|T} \end{pmatrix} = (M(X, Y)),$$

Phylogenetic Trees and Evolution

$M(X, Y) = P_{X|Y}$ is the probability that $X \in \{A, C, G, T\}$ at the node v_1 changes to $Y \in \{A, C, G, T\}$ at the node v_2 during the evolutionionary step represented by e.
M_e is a **stochastical matrix**. [4]

We have $P^{v_1} M_e = P^{v_2}$.

[4] The sum of the entries in a row of the matrix is 1, the sum of the entries of a column in the matrix is 1.

$M(X, Y) = P_{X|Y}$ is the probability that $X \in \{A, C, G, T\}$ at the node v_1 changes to $Y \in \{A, C, G, T\}$ at the node v_2 during the evolutionionary step represented by e.
M_e is a **stochastical matrix**. [4]

$$\text{We have } P^{v_1} M_e = P^{v_2}.$$

We write $v_1 = pa(v_2)$ and call v_1 the **parent** of v_2.

[4] The sum of the entries in a row of the matrix is 1, the sum of the entries of a column in the matrix is 1.

We write for the nodes $\mathcal{N}(\mathcal{T}) = \{1, \ldots, n, n+1, \ldots, N\}$ such that the leaves $\mathcal{L}(\mathcal{T}) = \{1, \ldots, n\}$ and N being the root. We assume that we have random variables $X_1, \ldots, X_N$ at the nodes taking values $x_1, \ldots, x_N \in \{A, C, G, T\}$ and write

$$P_{x_1,\ldots,x_n} = \mathrm{Prob}(X_1 = x_1, \ldots, X_n = x_n).$$

Gorilla	AAGCTTCACCGGCGCAGTTGTTCTTATAATTGCCCACGGACTTACATCAT
Cimpanzee	AAGCTTCACCGGCGCAATTATCCTCATAATCGCCCACGGACTTACATCCT
Human	AAGCTTCACCGGCGCAGTCATTCTCATAATCGCCCACGGGCTTACATCCT

$$P_{A,A,A} = \frac{\text{number of observations of AAA}}{\text{sequence length}} = \frac{10}{50} = \frac{1}{5}.$$

Phylogenetic Trees and Evolution

According to the Markov property of our process we obtain

$$P_{x_1,\ldots,x_n} = \sum_{\substack{(x_{n+1},\ldots,x_N) \\ x_s \in \{A,C,G,T\}}} P^N_{x_N} \prod_{v \in \mathcal{N}(\mathcal{T}) \setminus \{N\}} M_{(pa(v),v)}(x_{pa(v)}, x_v) \ .$$

Phylogenetic Trees and Evolution

According to the Markov property of our process we obtain

$$P_{x_1,\ldots,x_n} = \sum_{\substack{(x_{n+1},\ldots,x_N) \\ x_s \in \{A,C,G,T\}}} P^N_{x_N} \prod_{v \in \mathcal{N}(\mathcal{T}) \setminus \{N\}} M_{(pa(v),v)}(x_{pa(v)}, x_v) \ .$$

We obtain a map

$$\varphi_{\mathcal{T}} : \mathbb{R}^4 \times \prod_{e \in \mathcal{E}(\mathcal{T})} \mathbb{R}^{16} \longrightarrow \mathbb{R}^{4^n}$$

$$\varphi_{\mathcal{T}}(P^N, \ (\text{entries of } M_e)_{e \in \mathcal{E}(\mathcal{T})}) = (\ldots, P_{x_1,\ldots,x_n}, \ldots)$$

which we consider as before as a map over the complex numbers:

$$\varphi_{\mathcal{T}} : \mathbb{C}^4 \times \prod_{e \in \mathcal{E}(\mathcal{T})} \mathbb{C}^{16} \longrightarrow \mathbb{C}^{4^n} \ .$$

The choice of a special type of the matrices M_e and a distribution P^N for the root defines the model $\mathcal{M}$ choosen for the tree. If these matrices depend on d parameters and $\pi : \mathbb{C}^d \longrightarrow \mathbb{C}^4 \times \prod_{e \in \mathcal{E}(\mathcal{T})} \mathbb{C}^{16}$ defines this specification, we obtain the model map $\varphi_{\mathcal{T}}^{\mathcal{M}} = \varphi_{\mathcal{T}} \circ \pi$:

$$\varphi_{\mathcal{T}}^{\mathcal{M}} : \mathbb{C}^d \longrightarrow \mathbb{C}^{4^n} .$$

The **phylogenetic variety** according to the tree $\mathcal{T}$ and the model $\mathcal{M}$, $V_{\mathcal{M}}(\mathcal{T})$ is the Zariski closure of the image of $\varphi_{\mathcal{T}}^{\mathcal{M}}$ in $\mathbb{C}^{4^n}$.

Phylogenetic Trees and Evolution

There are many special models in evolutionary biology. We will give one example. The distribution at the root is usually choosen as $P^N = \{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$.

Phylogenetic Trees and Evolution

There are many special models in evolutionary biology. We will give one example. The distribution at the root is usually choosen as $P^N = \{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$.

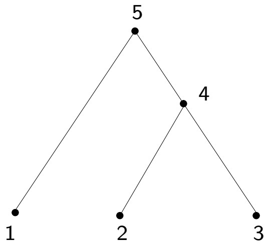
The **Jukes–Cantor model**

considers at the edges matrices of type

$$\begin{pmatrix} 1-3a & a & a & a \\ a & 1-3a & a & a \\ a & a & 1-3a & a \\ a & a & a & 1-3a \end{pmatrix}$$

Example

Let us consider the phylogenetic tree



such that the leaves $1, 2, 3$ correspond to Gorilla, Human, Chimpanzee. The the Jukes-Cantor model is given by the map

$$\varphi_T^{\mathcal{M}} : \mathbb{C}^4 \longrightarrow \mathbb{C}^{64} \ .$$

We want to compute now the ideal J of model invariants, $V(J) = \overline{\Im(\varphi_T^{\mathcal{M}})}$.

Example

We simplify the notations assuming that $\{A, C, G, T\}$ is identified with $\{1, 2, 3, 4\}$. Then we have (before specializing to the Jukes-Cantor model)

$$P_{ijk} = \sum_{l,m=1}^{4} P_m^5 M_{(5,1)}(i, m) M_{(5,4)}(l, m) M_{(4,2)}(j, l) M_{(4,3)}(k, l) \ .$$

Example

```
> ring JC=0,(p(1..4)(1..4)(1..4),a(1..4)),lp;
```

We create the ideal I associated to the map $\varphi_T^{\mathcal{M}}$ and eliminate the variables $a(1)$, $a(2)$, $a(3)$, $a(4)$ occuring in the 4 stochastic matrices $M_{(5,1)}$, $M_{(5,4)}$, $M_{(4,2)}$, $M_{(4,3)}$ to obtian the ideal J of the 61 model invariants.

```
> ideal J=eliminate(I,a(1)*a(2)*a(3)*a(4));
> J;
J[1]=p(4)(4)(2)-p(4)(4)(3)
J[2]=p(4)(4)(1)-p(4)(4)(3)
    [...]


J[55]=24*p(1)(2)(3)+12*p(4)(3)(3)+12*p(4)(3)(4)+12*p(4)(4)(3)
      +4*p(4)(4)(4)-1
J[56]=p(1)(2)(2)-p(4)(3)(3)
```

Example

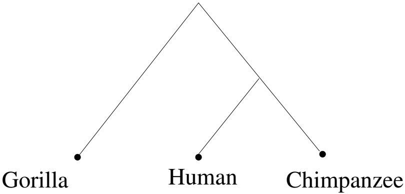
If we compare the parts of DNA for Gorilla, Human and Chimpanzee (from a part of length 1000), we observe $p_{1,1,1} = \frac{9}{50}$, $p_{4,3,3} = \frac{9}{500}$ and $p_{1,1,3} = \frac{3}{1000}$.

Example

If we compare the parts of DNA for Gorilla, Human and Chimpanzee (from a part of length 1000), we observe
$p_{1,1,1} = \frac{9}{50}$, $p_{4,3,3} = \frac{9}{500}$ and $p_{1,1,3} = \frac{3}{1000}$.
Using this observation we can compute the stochastic matrices.
There is one degree of freedom with respect to the 4 parameters of the matrices.
If we put $a_1 = 0.03$ we obtain $a_2 = 0.006$, $a_3 = 0.02$ and $a_4 = 0.05$.

Example

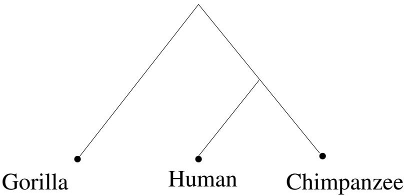
We can use the model invariants to decide about the topology of the tree. In our special situation we have 6 possibilities for Gorilla , Human and Chimpanzee.



We know than this tree is correct.

Example

We can use the model invariants to decide about the topology of the tree. In our special situation we have 6 possibilities for Gorilla , Human and Chimpanzee.



We know than this tree is correct.
If we exchange the Chimpanzee and the Gorilla in our model then we obtain a value for $p_{4,1,1} = \frac{3}{1000}$ which was not observed. Observed was $p_{4,1,1} = \frac{9}{500}$.