EUCLID, DESCARTES, STURM ET AL.: IN SEARCH OF THE REAL ROOTS OF POLYNOMIALS

(ORIGINAL TITLE: STURM SEQUENCES AND A DISCRIMINANT IN BIOLOGY)

Alexandru Iosif
Universidad
Rey Juan Carlos
(Madrid, Spain)

Theano
(Source:
Mujeresconciencia.com)

Euclidean division before Euclid

- "It is my judgment that this entire book (**Euclid’s Book VII**) should be attributed to the Pythagoreans before Archytas.”
  (van der Waerden, Science Awakening)

Archytas: teacher or disciple of Plato?

- “[…] and that he **[Plato]** spent a long time with Archytas of Tarentum and Timaeus of Locris, and got hold of the commentaries of Philolaus, and that, as the fame of Pythagoras dominated at that time and place, he devoted himself to the school of Pythagoras and to these studies.”
  (Cicero, De re publica)
- “[…] however, he was at first despised **[Archytas]** and owed his remarkable progress to studying with Plato.”
  (Demosthenes, Ἐρωτικός)

Euclid, Book VII

Proposition 1: *When two unequal numbers are set out, and the less is continually subtracted in turn from the greater, if the number which is left never measures the one before it until a unit is left, then the original numbers are relatively prime.*

Proposition 2: *To find the greatest common measure of two given numbers not relatively prime.*

Euclid's algorithm calculates the greatest common divisor (gcd) of two numbers.

Example: 24 and 14:

$24 - 14 = \mathbf{12}$, $14 - \mathbf{12} = \mathbf{2}$, $12 - 6 \cdot \mathbf{2} = \mathbf{0}$. Hence, $\gcd(24,14) = \mathbf{2}$.

Oxford University Museum of Natural History

(Source: Turismo Matemático)

¿What about other rings?

XIX and XX centuries:

- Guilty of extending this algorithm to other rings (Euclidean rings).
- XX Century: Guilty of the name Euclidean division (i.e., division with remainder in Euclidean rings).

Example: Consider the polynomials $\mathrm{P(x)} = x^5 + 2x^3 + x$ and $\mathrm{Q(x)} = x^4 - 1$. We can use the Euclid's algorithm to compute gcd(P, Q):

$$(x^5 + 2x^3 + x) - \mathrm{x}(\mathrm{x}^4 - 1) = \left(\mathbf{2x^3 + 2}\boldsymbol{x}\right),$$

$$(\mathrm{x}^4 - 1) - \frac{1}{2}x\left(\boldsymbol{2x^3 + 2x}\right) = \left(\boldsymbol{-x^2 - 1}\right),$$

$$(2\mathrm{x}^3 + 2x) - (-2x)\left(\boldsymbol{-x^2 - 1}\right) = \mathbf{0}.$$

Hence, gcd$(P, Q) = \boldsymbol{-x^2 - 1}$.

(Source: Blog de Matemáticas y TIC's)

Polynomials vs. integers

It seems polynomials behave as if they were integers.

"The study of increasingly abstract and complex domains did not shake the conviction, matured in the 19th century, that anything can be related to the simple concept of integer, while the integer, in turn, can be related to the even simpler concept of set."

(Zellini, The Mathematics of the Gods and the Algorithms of Men)

Sturm

Sturm (1829) introduces a variantion of the Euclidean division:

- We start by dividing a polynomial by its derivative.
- Instead of keeping the reminder of this division, we keep its negative.
- We keep doing it until we reach zero.

¿What do we get out of this?

A method for counting the real roots of a polynomial in any interval.

Porträt des jungen Wissenschaftlers. Öl auf Leinwand von François d'Albert-Durade nach einer 1822 angefertigten Skizze von Sturms Kollege Jean-Daniel Colladon (Bibliothèque de Genève).

Descartes
(Source: Wikimedia Commons)

Descartes' rule of signs

- An algorithm proposed by Descartes in 1637 (without proof).
- It bounds the number $n_+(p)$ of positive roots of any polynomial p in an interval:

$$n_+(p) \leq N(p), \qquad \text{with} \quad n_+(p) \equiv N(p) \pmod 2,$$

where $n_+(p)$ is to be counted with multiplicity and $N(p)$ denotes the number of sign changes of the coefficients of p.

Example: $\mathrm{p} = x^3 + x + 1$ does not have positive roots since $N(p) = 0$.

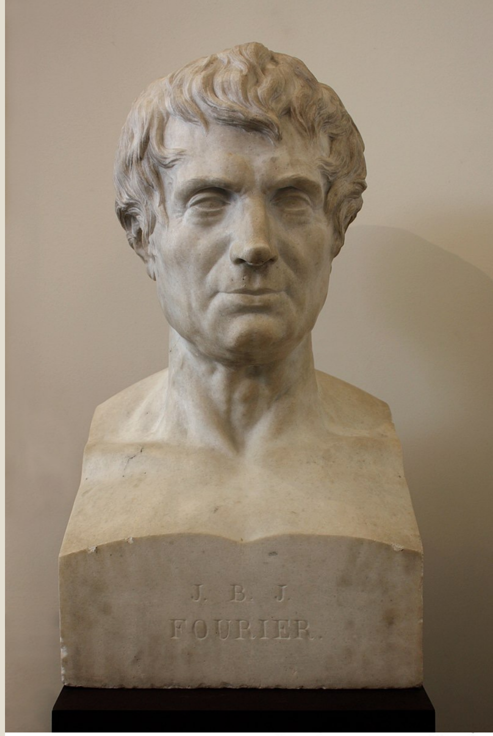
With a *linear fractional transformation*, we can bound the number of roots in any interval:

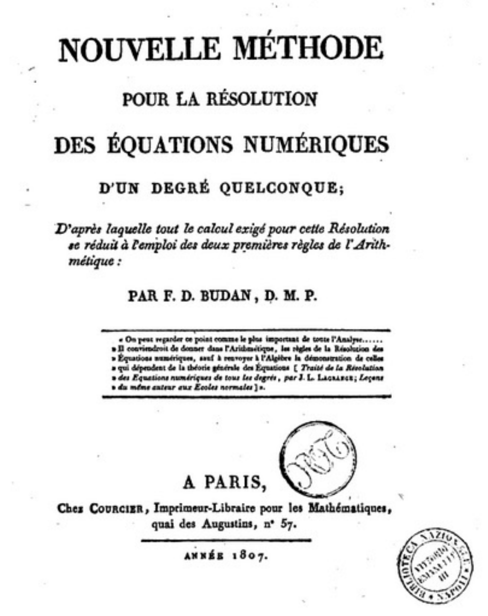
$$x \mapsto \frac{ax+b}{cx+d}, \qquad \textit{where } ad - bc \neq 0.$$

(This is ***Budan-Fourier Theorem****.)*

Example: With the transformation $x \mapsto -x$, we bound the number of negative roots:

$$n_- \leq N(p(-x)), \qquad \text{con}\; n_-(p) \equiv N(p(-x)) \pmod 2$$




NOUVELLE MÉTHODE

POUR LA RÉSOLUTION

DES ÉQUATIONS NUMÉRIQUES

D'UN DEGRÉ QUELCONQUE;

D'après laquelle tout le calcul exigé pour cette Résolution se réduit à l'emploi des deux premières règles de l'Arithmétique :

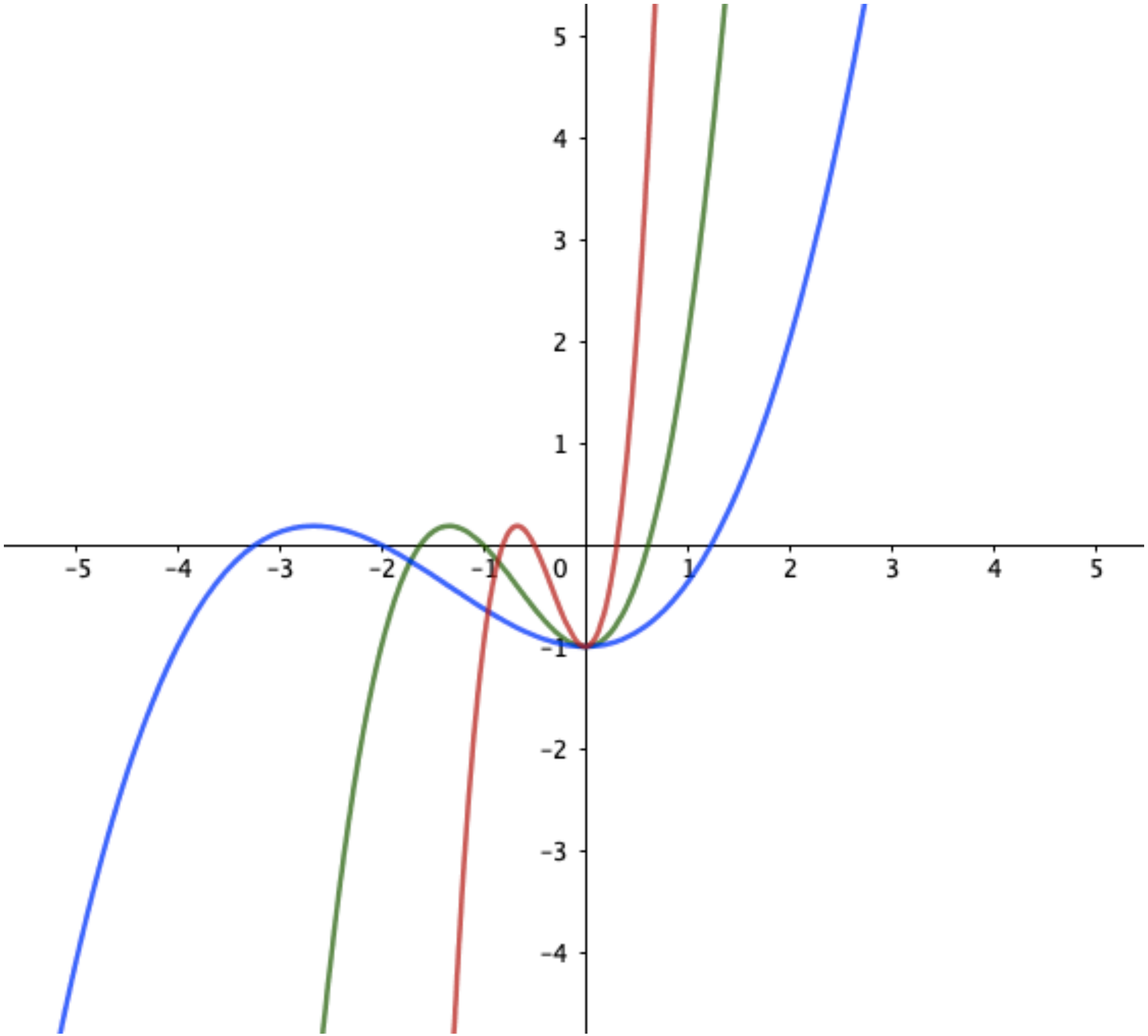
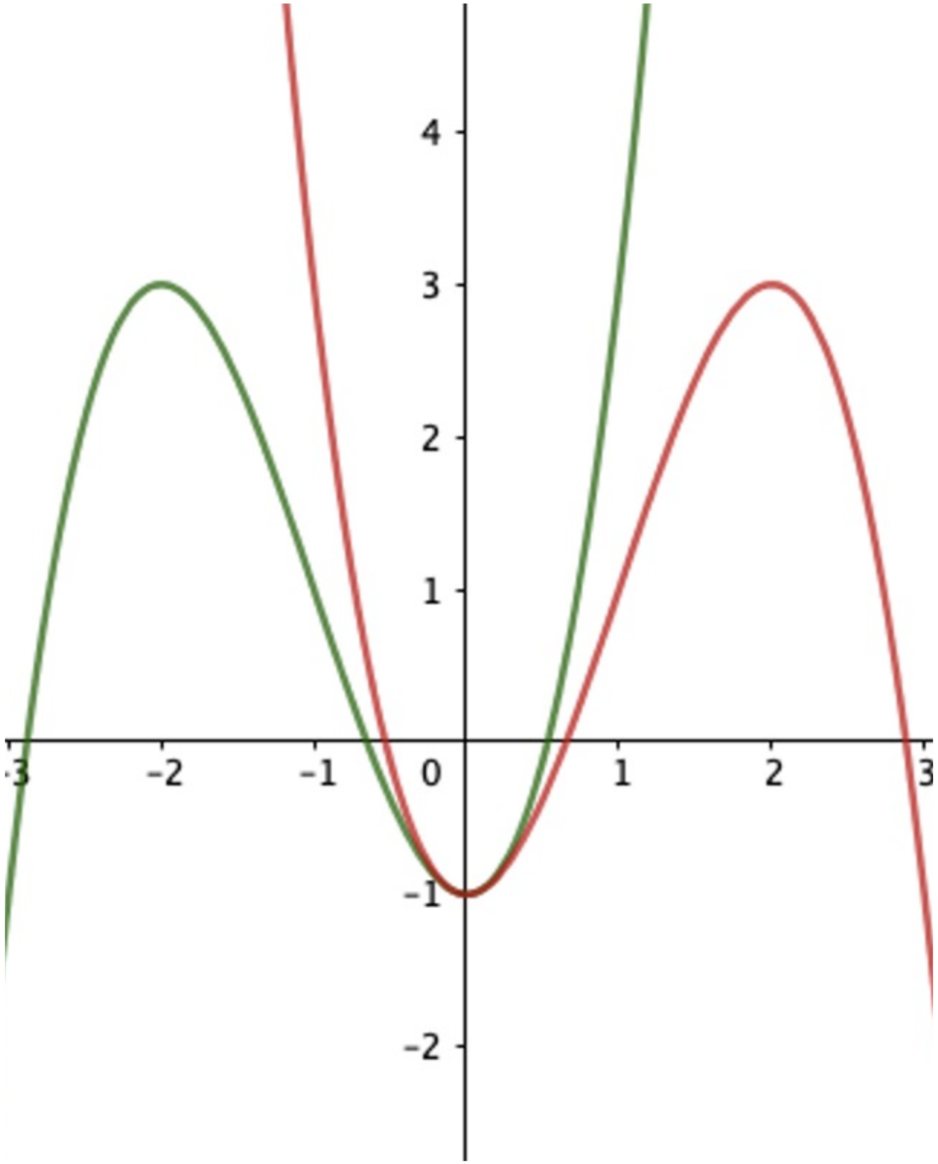
PAR F. D. BUDAN, D. M. P.

A PARIS,

Chez COURCIER, Imprimeur-Libraire pour les Mathématiques, quai des Augustins, n° 57.

ANNÉE 1807.

Fourier and Budan
(Source: Wikimedia Commons)


-5 -4 -3 -2 -1 0 1 2 3 4 5
5 4 3 2 1 -1 -2 -3 -4

-3 -2 -1 0 1 2 3
4 3 2 1 -1 -2

On connoiſt auſſy de cecy combien il peut y auoir de vrayes racines, & combien de fauſſes en chaſque Equation. A ſçauoir il y en peut auoir autant de vrayes, que les ſignes $+$ & $--$ s'y trouuent de fois eſtre changés ; & autant de fauſſes qu'il s'y trouue de fois deux ſignes $+$, ou deux ſignes $--$ qui s'entreſuiuent. Comme en la derniere, a cauſe qu'aprés $+x^4$ il y a $-- 4x^3$, qui eſt vn changement du ſigne $+$ en $--$, & aprés $-- 19xx$ il y a $+ 106x$, & aprés $+ 106x$ il y a $-- 120$ qui ſont encore deux autres changemens, on connoiſt qu'il y a trois vrayes racines; & vne fauſſe, a cauſe que les deux ſignes $--$, de $4x^3$, & $19xx$, s'entreſuiuent.

Combien il peut y auoir de vrayes racines en chaſque Equatiõ.

"We can determine also the number of true and false roots that any equation can have, as follows: An equation can have as many true roots as it contains changes of sign, from + to - or from - to +; and as many false roots as the number of times two + signs or two - signs are found in succession."

Dictionary:
true root = positive root
false root = negative root

Ex libris Congreg. Missionis Domus Cenomanensis

LA
GEOMETRIE.
DE
RENÉ DESCARTES.

A PARIS,
Chez CHARLES ANGOT, ruë ſaint Iacques, au Lion d'or.

M. DC. LXIV.
AVEC PRIVILEGE DV ROY.

Example:
Show that the following polynomial has exactly one real root:
$$p(x) = x^5 + 1.$$
Solution:
First, note that $p(x)$ has no positive root, since $N(p(x)) = 0$. Also note that 0 is not a root. Then, observe that $p(-x) = -x^5 + 1$, meaning that
$$N\big(p(-x)\big) = 1 = n_+(p(-x)).$$
Finaly, note that $n_-(p(x)) = n_+(p(-x))$. Hence, $p(x)$ has exactly one real root.

Example:
Show that, by using only Descartes' rule of signs for $p(x)$ and $p(-x)$ we cannot determine the exact number of real roots of the following polynomial
$$p(x) = x^3 + x^2 + x + 1.$$
Solution:
First, observe that $N\big(p(x)\big) = 0$, and, therefore, $p(x)$ has no positive root. Also observe that 0 is not a root.
Then, observe that $p(-x) = -x^3 + x^2 - x + 1$. So, $N\big(p(-x)\big) = 3$. Hence, $p(x)$ has either 1 or 3 negative roots. In conclusion, we cannot determine, by using only this algorithm, the exact number of real roots of this polynomial.

Sturm
(Source: Wikimedia Commons)

Sturm sequences

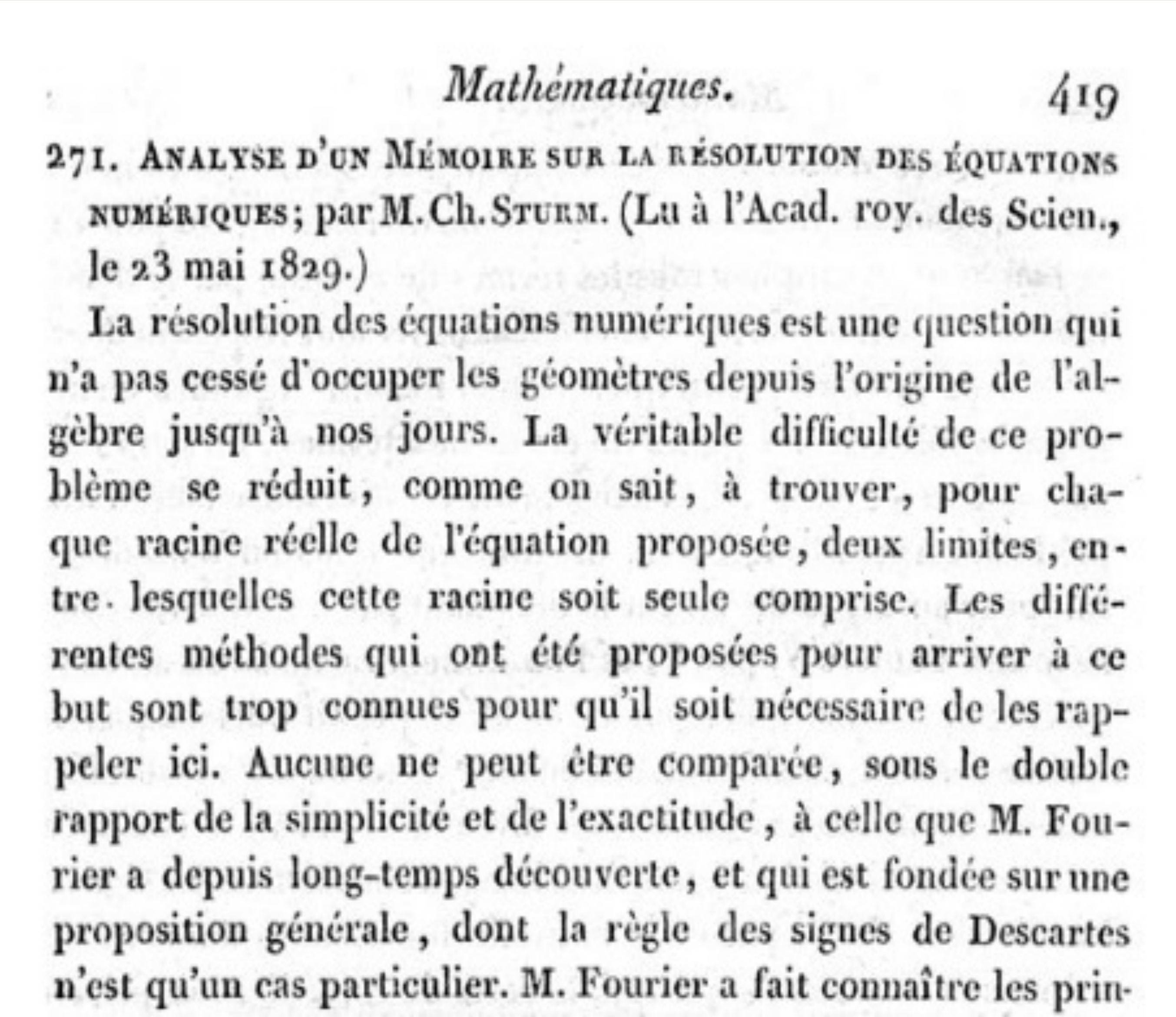
- The Sturm sequence $S(p)$ of $p(x)$ is a sequence of nonzero polynomials $(s_0, s_1, s_2, \dots)$ depending on $p(x)$, where:

$$s_0 = p(x),$$
$$s_1 = p'(x),$$
$$s_i = -\text{rem}\,(p_{i-2}, p_{i-1}).$$

- Given an arbitrary number $a \in \mathbb{R} \cup \{\pm\infty\}$, by $\chi_p(a)$ we denote the number of sign changes of the following sequence:

$$(s_0(a), s_1(a), s_2(a), \dots).$$

Sturm’s Theorem (Jacques Charles François Sturm; 1829)*:



Mathématiques. 419

271. ANALYSE D'UN MÉMOIRE SUR LA RÉSOLUTION DES ÉQUATIONS NUMÉRIQUES; par M. Ch. STURM. (Lu à l'Acad. roy. des Scien., le 23 mai 1829.)

La résolution des équations numériques est une question qui n'a pas cessé d'occuper les géomètres depuis l'origine de l'algèbre jusqu'à nos jours. La véritable difficulté de ce problème se réduit, comme on sait, à trouver, pour chaque racine réelle de l'équation proposée, deux limites, entre lesquelles cette racine soit seule comprise. Les différentes méthodes qui ont été proposées pour arriver à ce but sont trop connues pour qu'il soit nécessaire de les rappeler ici. Aucune ne peut être comparée, sous le double rapport de la simplicité et de l'exactitude, à celle que M. Fourier a depuis long-temps découverte, et qui est fondée sur une proposition générale, dont la règle des signes de Descartes n'est qu'un cas particulier. M. Fourier a fait connaître les prin-

Let $p(x)$ be a real polynomial. Then, the number of distinct real roots of $p(x)$ in an interval (a, b), where $a, b \in \mathbb{R} \cup \{\pm\infty\}$, is equal to

$$|\chi_p(a) - \chi_p(b)|.$$

*For a proof, see Section 2.2.2 in [Basu].

Example:

Compute the exact number of real roots of the following polynomial

$$p(x) = x^3 + x^2 + x + 1.$$

Solution:

We start by computing the Sturm sequence of this polynomial:

$$s_0 = p(x) = x^3 + x^2 + x + 1,$$
$$s_1 = p'(x) = 3x^2 + 2x + 1,$$
$$s_2 = -\text{rem}\,(s_0, s_1) = -\frac{4}{9}x - \frac{8}{9},$$
$$s_3 = \ -\text{rem}\,(s_1, s_2) = -9.$$

Now, since we want to compute the number of real roots of $p(x)$, we need to compute $\chi(\infty)$ and $\chi(-\infty)$:

$$\chi(-\infty) = (-\infty, +\infty, +\infty, -9) = 2,$$

$$\chi(+\infty) = (+\infty, +\infty, -\infty, -9) = 1.$$

We conclude that $p(x)$ has $|\chi(-\infty) - \chi(+\infty)| = |2 - 1| = 1$ real roots.

Semialgebraic sets

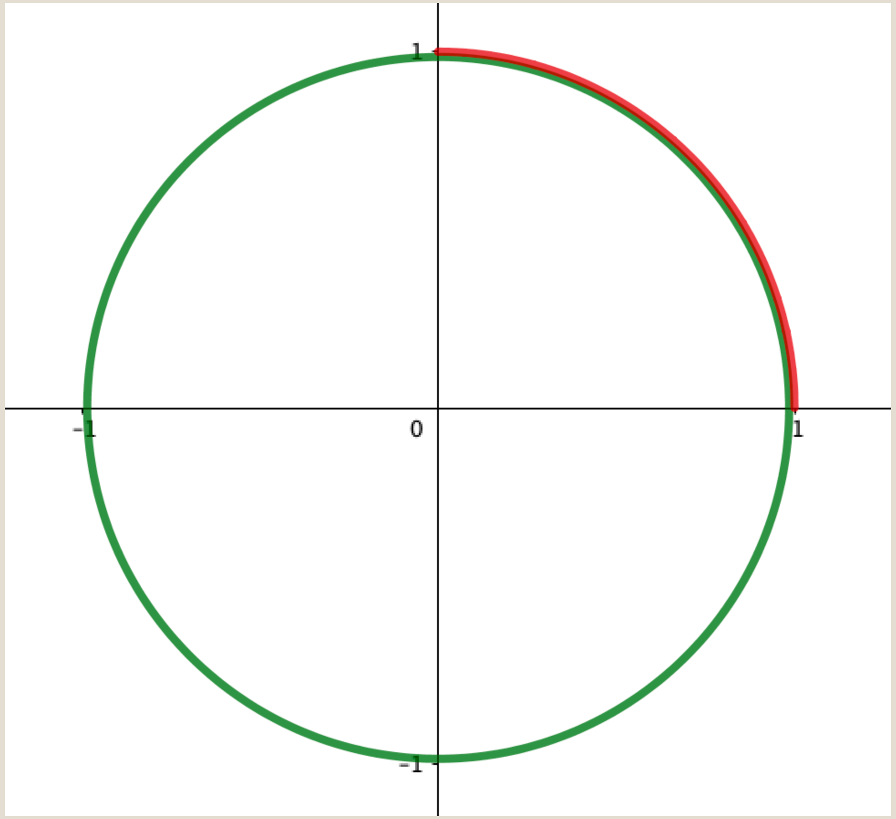
Definition:

A **basic semialgebraic** set is a set defined by (univariate or multivariate) polynomial equalities and polynomial inequalities. A **semialgebraic set** is a finite union of basic semialgebraic sets.

Example

The locus of the equation $x^2 + y^2 - 1 = 0$ is the circle of radius 1 centred at the origin (green). This set is algebraic.

Now, if we want the set of nonnegative solutions to this equation, we will obtain only a quarter of the previous circle (red). This set is not algebraic anymore; it is a basic semialgebraic set.

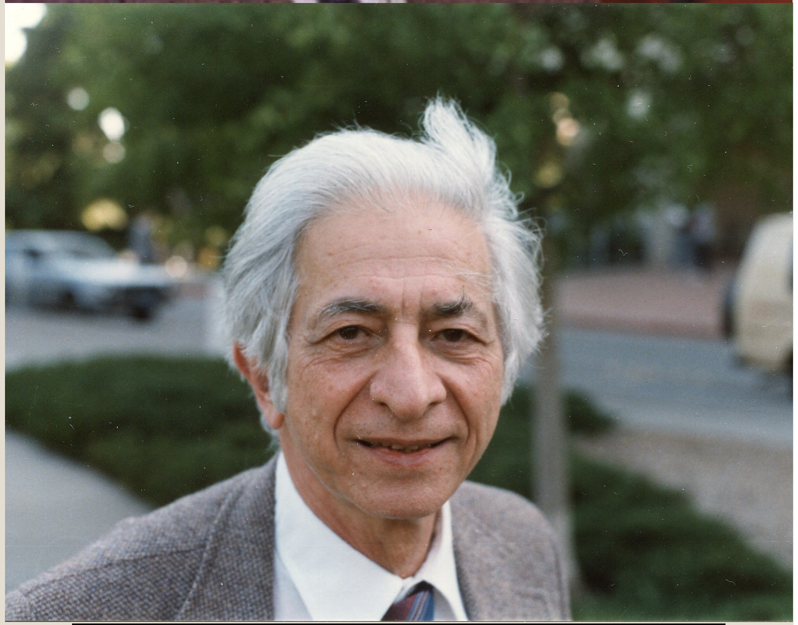


Tarski-Seidenberg Theorem

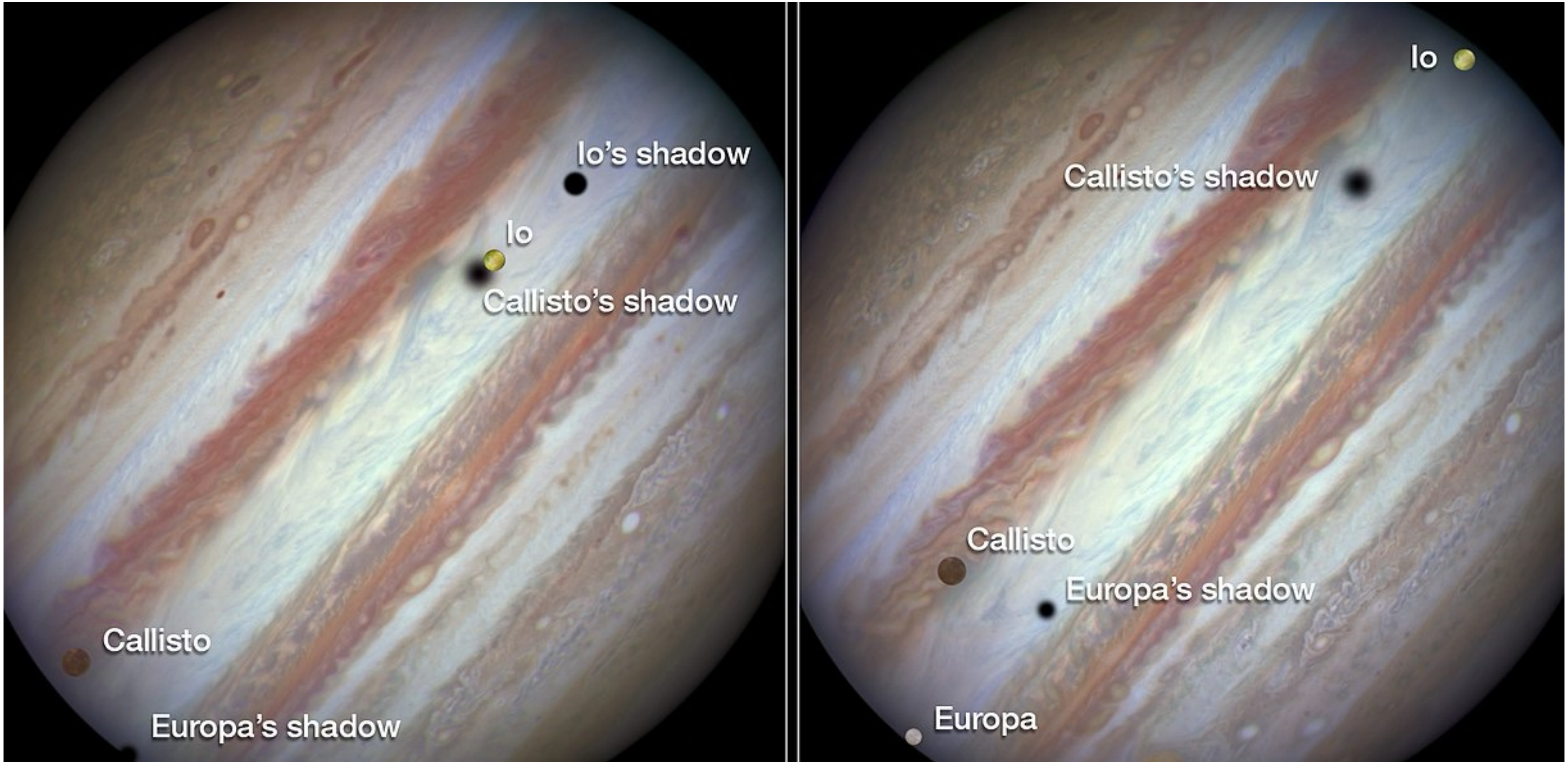
Theorem (Tarski-Seidenberg, first half of XX century)
Given a semialgebraic set in n+1 dimensions, it can be projected to an n dimensional space, and the result is still semialgebraic.

Observation
The original proof is constructive, essentially through Sturm sequences. The corresponding algorithm is too complex in most cases, and better algorithms exist. However, we show that, in a very special case, this algorithm might work.

Application
"Number of roots" in larger dimensions.



Alfred Tarski & Abraham Seidenberg
(Source: Wikimedia Commons)

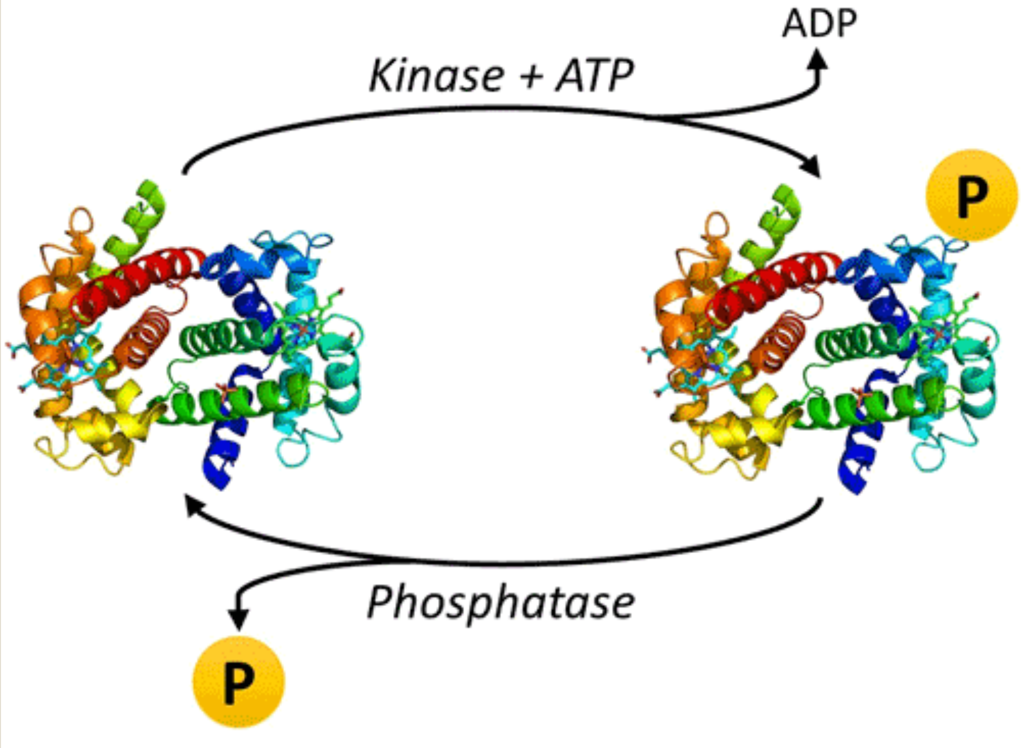


Source: Wikimedia Commons

An application to Biology

- Some molecular interactions can be described as polynomial ODEs:

$$\begin{cases} \dot{x}_1 & = P_1(k_1, \ldots, k_r; x_1, \ldots, x_n), \\ \vdots & \\ \dot{x}_n & = P_n(k_1, \ldots, k_r; x_1, \ldots, x_n), \end{cases}$$



- If we are only interested in steady states, we can set

$$\dot{x_1} = \dot{x_2} = \cdots = \dot{x_n} = 0,$$

thus, obtaining polynomial equations.

- Now, trying to classify the parameters k with respect to the number of positive roots is some kind of projection.

$$S + K \underset{k_2}{\overset{k_1}{\rightleftharpoons}} SK \xrightarrow{k_3} S_p + K \underset{k_5}{\overset{k_4}{\rightleftharpoons}} S_pK \xrightarrow{k_6} S_{pp} + K$$

$$S_{pp} + P \underset{k_8}{\overset{k_7}{\rightleftharpoons}} S_{pp}P \xrightarrow{k_9} S_p + P \underset{k_{11}}{\overset{k_{10}}{\rightleftharpoons}} S_pP \xrightarrow{k_{12}} S + P$$

$$\begin{aligned}
[\dot{S}] &= -k_1[S][K] + k_2[SK] + k_{12}[S_pP] \\
[\dot{K}] &= -k_1[S][K] + (k_2 + k_3)[SK] - k_4[K][S_p] + (k_5 + k_6)[S_pK] \\
[\dot{SK}] &= k_1[S][K] - (k_2 + k_3)[SK] \\
[\dot{S_p}] &= k_3[SK] - k_4[K][S_p] + k_5[S_pK] + k_9[S_{pp}P] - k_{10}[S_p][P] + k_{11}[S_pP] \\
[\dot{S_pK}] &= k_4[K][S_p] - (k_5 + k_6)[S_pK] \\
[\dot{S_{pp}}] &= k_6[S_pK] - k_7[S_{pp}][P] + k_8[S_{pp}P] \\
[\dot{P}] &= -k_7[S_{pp}][P] + (k_8 + k_9)[S_{pp}P] - k_{10}[S_p][P] + (k_{11} + k_{12})[S_pP] \\
[\dot{S_{pp}P}] &= k_7[S_{pp}][P] - (k_8 + k_9)[S_{pp}P] \\
[\dot{S_pP}] &= k_{10}[S_p][P] - (k_{11} + k_{12})[S_pP].
\end{aligned}$$

a[4]^7-2700*a[1]*a[2]^3*a[3]^2*a[5]^4+2160*a[1]*a[2]^3*a[3]*a[4]^2*a[5]^3-432*a[1]*a[2]^3*a[4]^4*a[5]^2+1800*a[1]*a[2]^2*
5]^4-9600*a[0]*a[1]*a[2]*a[4]^4*a[5]^3+26000*a[0]*a[1]*a[3]^3*a[4]*a[5]^4-26400*a[0]*a[1]*a[3]^2*a[4]^3*a[5]^3+8640*a[0]*a
a[1]^3*a[3]^2*a[5]^5-25600*a[1]^3*a[3]*a[4]^2*a[5]^4+5120*a[1]^3*a[4]^4*a[5]^3-26400*a[1]^2*a[2]*a[3]^2*a[4]*a[5]^4+21120
a[3]^2*a[4]^5*a[5]+448*a[1]*a[2]*a[3]*a[4]^7+2400*a[1]*a[3]^6*a[5]^3-2520*a[1]*a[3]^5*a[4]^2*a[5]^2+864*a[1]*a[3]^4*a[4]^

*a5*a7*c2,a[2]=2*a1*a2^2*a5^3*c1*c2+a1*a2^2*a5^3*c2^2-2*a1*a2*a4*a5^3*c1^2-a1*a4^2*a5^3*c1^2-a1^2*a2*a5^3*c2+a1^2*a3*a5^2
a6^2*c2^2+2*a1*a3*a4^2*a5^2*c1^2+4*a1*a3*a4^2*a5^2*c1*c2-2*a1*a3*a4*a5^2*a6*c2^2+a1^2*a3*a4*a5^2*c2+a1*a2*a3*a4*a5^2*c2-a1
*c1-a1^2*a3*a5^2*a6*c2+a1^2*a4*a5^3*c2+a1*a2*a3*a4*a5^2*c1-a1*a2*a3*a5^3*c2-2*a1*a2*a3*a5^2*a6*c2+a1*a2*a3*a5^2*a7*c1+a1*

2],3*a[3],4*a[4],5*a[5],25*a[5],4*(5*a[3]*a[5]-2*a[4]^2)^2,25*a[5]*(-75*a[0]*a[2]*a[5]^2+55*a[0]*a[3]*a[4]*a[5]-16*a[0]*a[

References:

- Basu, S., Pollack, R., Roy, M.-F (2008). *Algorithms in Real Algebraic Geometry*, Publisher: Springer-Verlag, Second edition.
- Descartes, R (1886). *La géométrie*. Hermann.
- van den Dries, L. (1988). *Alfred Tarski's elimination theory for real closed fields*. The Journal of Symolic Logic. 53.1: 7-19.
- Iosif, A. (2019): *Algebraic Methods for detecting multistationarity in mass-action networks*. PhD Thesis.
- Sturm, J.C.F. (1829). *Mémoire sur la résolution des équations numériques. Bulletin des Sciences de Férussac.* ***11****: 419–425.*
- van der Waerden, B. L (1961). *Science Awakening*, Publisher: Oxford University Press.
- Zellini, P. (2016/2018). *La matemática de los dioses y los algoritmos de los hombres*. Siruela.

Thank you!

¡Gracias!

Vă mulțumesc!