WIT: A symbolic system for computations in IT and EG (programmed in pure Python)

13-17/01/2020

S. Xambó

UPC/BSC · IMUVA

& N. Sayols & J.M. Miret

WIT: Un sistema simbólico programado en Python para cálculos de teoría de intersecciones y geometría enumerativa

En este curso se entrelazan cuatro temas principales que aparecerán, en proporciones variables, en cada una de las sesiones:

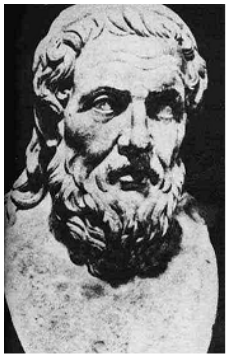
(1) Repertorio de problemas de geometría enumerativa y el papel de la geometría algebraica en el enfoque de su resolución.

(2) Anillos de intersección de variedades algebraicas proyectivas lisas. Clases de Chern y su interpretación geométrica. Descripción explícita de algunos anillos de intersección paradigmáticos.

(3) Enfoque computacional: Su interés y valor, principales sistemas existentes. WIT (filosofía, estructura, potencial). Muestra de ejemplos tratados con WIT.

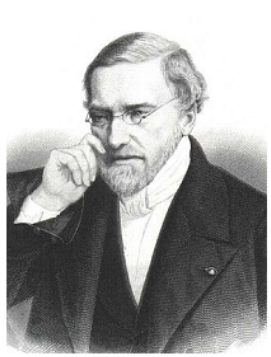
(4) Perspectiva histórica: Galería de héroes, hitos más significativos, textos y contextos, quo imus?

Index


Apollonius

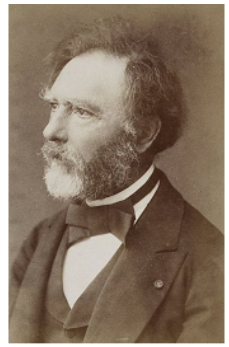

Descartes


Bézout


Poncelet


Steiner


Plücker

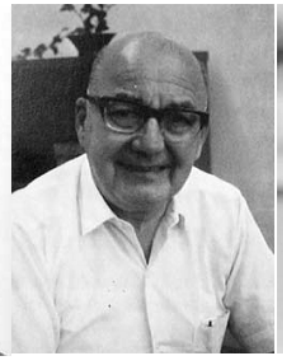

Puiseux


Zeuthen

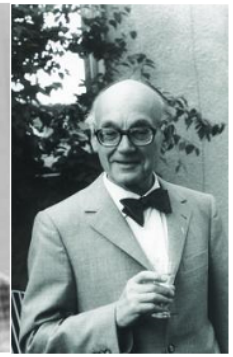

Lie


Schubert

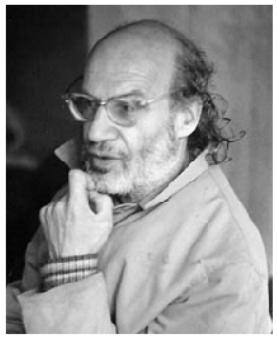

Klein


Hasse

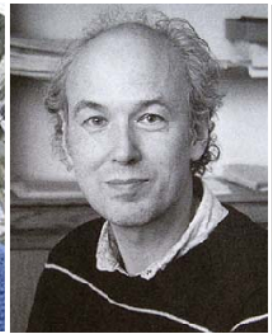

Weil


Deuring


Serre


Grothendieck


Fulton


Deligne


Vainsencher

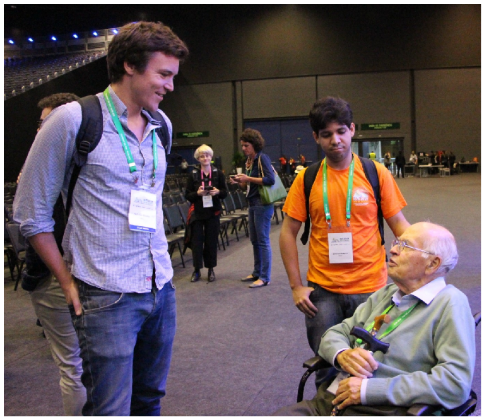

Strømme


Kontsevich

Apollonius from Perga (-262 – -190), René **Descartes** (1596-1650), Étienne **Bézout** (1730-1783), Jean-Victor **Poncelet** (1788-1867), Jakob **Steiner** (1796-1863), Julius **Plücker** (1801-1868), Victor **Puiseux** (1820-1883), Hieronymus **Zeuthen** (1839-1920), Sophus **Lie** (1842-1899), Hermann **Schubert** (1848-1911), Felix **Klein** (1849-1925), Helmut **Hasse** (1898-1979), André **Weil** (1906-1998), Max **Deuring** (1907-1984), Jean-Pierre **Serre** (1926-), Alexander **Grothendieck** (1928-2014), William **Fulton** (1939-), Pierre **Deligne** (1944-), Israel **Vainsencher** (1948-), Stein A. **Strømme** (1951-2014), Maxim **Kontsevich** (1964-).

Michael Atiyah, *in memoriam*

The mysterious ж. Bernoulli and Todd numbers. Higher order Bernoulli numbers. Comments of ж. A. Connes tribute.





Above: Atiyah at the ICM-2018 (Rio), center with I. Deaubechies, right with R. Pandharipande. Below: In Barcelona, April 2008, with mathematics students and DHC lecture.

In the preprint *The fine structure constant* (Atiyah 2018) we find these two expressions for Ж, the supposed mathematical formula for the inverse $1/\alpha$ of the *fine structure constant* α:

$$Ж = \lim_{n\to\infty,\ j\to\infty} 2^{-2n} B^n_{k(j)}, \quad k(j) = 2^{k(j-1)}, k(0) = 1,$$

where $B^n_{k(j)} = B(n, k(j))$ is a 'higher order' Bernoulli number, and

$$Ж == \frac{\pi}{\gamma \log 2} \lim_{n\to\infty} \sum_{j=1}^{n} \frac{1}{2^{j+1}} (j \log j - j + \frac{\log j + 1}{j}).$$

Remark: Also called *Sommerfeld constant*, α is the dimensionless physical quantity

$$\alpha = \frac{1}{4\pi\varepsilon_0} \frac{e^2}{\hbar c}, \quad \text{and} \quad 1/\alpha = 137.035999084(21).$$

Remark: $k(j)$ is superexponential in j: $k(0) = 1$, $k(1) = 2$, $k(2) = 2^2$, $k(4) = 2^{2^2} = 16$, $k(5) = 2^{16} = 65536$, $k(6) = 2^{65536}$ (19729 decimal digits), ...

The *Bernoulli numbers* B_n $(n \geqslant 0)$ by

$$\frac{t}{e^t - 1} = \sum_{n \geqslant 0} \frac{B_n}{n!} t^n.$$

Similarly, the *Todd numbers* T_n $(n \geqslant 0)$ are defined by

$$\frac{x}{1 - e^{-x}} = \sum_{n \geqslant 0} T_n x^n.$$

Therefore, $T_n = (-1)^n B_n / n!$, or $B_n = (-1)^n n!\, T_n$.

Problem: To compute

$$t/(e^t - 1) = 1/(1 + x/2! + x^2/3! + \cdots + x^n/(n+1)! + \cdots$$

to any prescribed order.

Given a list or vector $[c_1, ..., c_r]$, and an integer $d \geqslant 0$, this function computes the list or vector of the first d coefficients, starting with degree 1, of the power series $(1 + c_1 t + \cdots + c_r t^r)^{-1}$, which is equivalent to find the inverse of $1 + c_1 t + \cdots + c_r t^r \bmod t^{d+1}$. By default, $d = r$.

```
def invert_vector(c, d=''):
    if isinstance(c,Vector_type):
        return vector(invert_vector(list(c),d))
    if len(c)==0: return invert_vector([0],d)
    if d==0: return []
    if d=='': d=len(c)
    c = pad(c,d)
    s = [-c[0]]
    if d==1: return s
    for k in range(1,d):
        s += [-c[k]-convolution(s,c,k-1)]
    return s
```

```
def bernoulli_numbers(N):
    u = 1>>Q_
    if N==0: return [u]
    B = invert_vector([u/factorial(j+1)\
           for j in range(1,N+1)])
    return [u]+[factorial(k+1)*B[k] for k in range(N)]
BV_ = bernoulli_numbers

def bernoulli_number(N):
    if N==0: return 1>>Q_
    elif N==1: return -1/2>>Q_
    else:
        if odd(N): return 0>>Q_
        else: return bernoulli_numbers(N)[-1]
B_=bernoulli_number
```

vprod(x,y,d)

If vecctors x and y have lengths r and s, this fucntion returns the first d components of the vector of coefficients, starting with degree 1, of the t-polynomial $(1 + x_1 t + \cdots + x_r t^r)(1 + y_1 t + \cdots + y_s t^s)$. By default, $d = r + s$.

vpower(x,m,d)

Returns the vector of the first d coefficients, starting with degree 1, of the t-polynomial $(1 + x_1 t + \cdots + x_r t^r)^m$. By default, $d = rm$.

```
def high_bernoulli_numbers(N,k):
    u = 1>>Q_
    if N==0: return [u]
    B = invert_vector([u/factorial(j+1)\
           for j in range(1,N+1)])
    B = vpower(B,k,N)
    return [u]+[factorial(j+1)*B[j] for j in range(N)]
#
HBs_=high_bernoulli_numbers

def HB_(n,k): return HBs_(n,k)[-1]
```

About ж

From a message to MA, Sep 2018, Sat 22

In [1] I find the formula (8.11) for ж:

$$(*) \qquad \text{ж} = \lim_{\substack{n\to\infty \\ j\to\infty}} 2^{-2n} B^n_{k(j)}$$

with j coprime with $2n$, $k(1) = 1$ and $k(j+1) = 2^{k(j)}$ for $j > 0$, and B^n_k the "Bernouilli numbers of higher order".

Since there are several conventions to denote Bernoulli numbers, particularly for the ordinary ones, does the definition of B^n_k above coincide with the definition you use?

As I understand it, the first few higher orders to care about are, according to $(*)$, the following:

j	1	2	3	4	5	6
$k(j)$	1	2	4	16	65536	2^{65536}

[1] M. Atiyah: "The fine structure constant". Preprint 2018-09-22.

[2] M. Atiyah: "The Riemann Hypothesis". Preprint 2018-09-22.

Answer Sun, 23 Sep: I will respond to your questions and comments later...

```
def zhe(n,j):
    if igcd(j,2*n)!=1:
        return 'zhe: coprime condition not satisfied'
    k=0
    for _ in range(j):
        k=2**k
    return HB_(n,k)/(2**(2*n))

N = [n for n in range(1,20) if igcd(n,3)==1 and igcd(n,5)

for n in N: print(abs(zhe(n,3)))

for n in N: print(abs(zhe(n,5)))
```

Remark: Only for $j = 3, 5$ (in which case n is required to be coprime with 3 and 5) can we actually compute the numbers, and the values you get are very small for $j = 3$ and very large for $j = 5$.

What about the other formula?

```
from math import pi,log
euler_gamma=0.577215664901532
kappa = pi/euler_gamma/log(2)

def atiyah(n):
    def t(j):
        x = (j*log(j)-j+(log(j)+1)/j)/log(2)
        return (1-x)/2**(j+1)
    s = sum([t(j) for j in range(1,n+1)])
    return s*kappa

print(atiyah(50)) => 0.23120602303795385
print(atiyah(100)) => 0.23120602303718477
print(atiyah(150)) => 0.23120602303718477
```

On an idea of Michael Atiyah

Alain Connes

January 31, 2019

In memoriam Michael Atiyah,
with admiration and gratitude

"In the broad light of day mathematicians check their equations and their proofs, leaving no stone unturned in their search for rigour. But, at night, under the full moon, they dream, they float among the stars and wonder at the miracle of the heavens. They are inspired. Without dreams there is no art, no mathematics, no life."

(Michael Atiyah, Les Déchiffreurs 2008, Notices of the AMS, 2010).

1 Introduction

The Feit–Thompson theorem on the solvability of finite groups of odd order was very much on Michael Atiyah's mind during his participation in the 2017 Shanghai conference on noncommutative geometry. Michael's lively presence there, and his inexhaustible enthusiasm for all mathematics –old, new and yet to be created– were highlights of the meeting.

The goal of the present paper, as a tribute to a luminous mathematical imagination that never dimmed, is to take seriously his proposal and to show that, understanding it in a broader sense, one arrives at a very interesting idea.

0. Installation of PyM

1. Carlitz congruences

$$B(p+2,p+1) \equiv 0 \mod p^2, p \geqslant 3, p \text{ prime.}$$

$$B(p+2,p+1) \equiv 0 \mod p^3, p \geqslant 5, p \text{ prime.}$$

$$B(p,p) \equiv \tfrac{1}{2}p^2 \mod p^3, p \geqslant 3, p \text{ prime.}$$

In the next congruences, $p > 3$:

$$B(p+1,p) \equiv -p\frac{B_{p+1}}{p+1} + \frac{1}{24}p^2 \mod p^3,$$

$$B(p+2,p) \equiv p^2\frac{B_{p+1}}{p+1} \mod p^4,$$

$$B(p+1,p+1) \equiv \frac{B_{p+1}}{p+1} - \frac{1}{24}p \mod p^2,$$

$$B(p^r,p) \equiv -\tfrac{1}{2}p^{r+1}(p-1)B_{p^r-1} \mod p^{r+2}.$$

2. Asymptotics of B_n

$$(-1)^{n+1}B_{2n} \sim \frac{2(2n)!}{(2\pi)^{2n}} \sim 4\sqrt{\pi n}\left(\frac{n}{\pi e}\right)^{2n}.$$

3. Euler numbers and Euler polynomials

$$\frac{2e^t}{e^{2t}+1} = 1 + \sum_{n\geqslant 1} E_n \frac{t^n}{n!} \quad (E_{2n+1} = 0, \quad (-1)^n E_{2n} > 0).$$

$$E_n(x) = \sum_{k=0}^{n} \binom{n}{k} \frac{E_k}{2^k} (x - \tfrac{1}{2})^{n-k}.$$

4. Continuous fractions. Check that the continuous fraction development of ϕ^3, $\phi = (1+\sqrt{5})/2$, is $[4, 4, 4, 4, ...]$. Find the first 10 rational approximations of ϕ^3.

Foreword

Materials and motivations. A short sample of enumerative problems. General pattern for solving enumerative problems: moduli, calculus of geometric conditions, effective computations. Lines meeting four lines in $\mathbb{P}^3$.

Access to these slides:

`https://mat-web.upc.edu/people/sebastia.xambo/ITEG/s-wit-pdf`

or via

`https://mat-web.upc.edu/people/sebastia.xambo/Talks.html`

Access to **PyM** and related resources:

`https://mat-web.upc.edu/people/sebastia.xambo/PyM.html`

Main motivation:

A hands-on free computational support for **UIT** and **UIT2** (see [33] and [35]):

`https://mat-web.upc.edu/people/sebastia.xambo/PyWIT.html`

The link ITEG in PyWIT opens de file ITEG-Book.html, which provides a way to access the witlets according to the context of the **UIT2** book.

- *Circles tangent to three given circles in the plane* (Apollonius)
- *Lines meeting 4 lines in* $\mathbf{P}^3$
- *Lines meeting 6 planes in* $\mathbf{P}^4$
- *Lines contained in a cubic in* $\mathbf{P}^3$
- *Lines contained in 5ic in* $\mathbf{P}^4$
- *Conics tangent to 5 conics in the plane*
- *Conics in* $\mathbf{P}^3$ *meeting 8 lines*
- *Conics contained in a 5ic in* $\mathbf{P}^4$

How many objects of a given type satisfy a given set of conditions, provided the number is finite?

If this number is infinite, it is usually interesting to add other conditions that allow us to get useful information about the space of solutions.

- *The moduli problem*: Find a *parameter space* $\mathcal{M}$ for the objects of the type we are interested in.

The moduli space is known by other names in other contexts, as for example *configuration space* in physics or in robotics, in which case the dimension of $\mathcal{M}$ is called (number of) *degrees of freedom* (DoF), or simply *freedom* of the system.

- *Calculus of conditions*: Interpret each condition in terms of the geometry of $\mathcal{M}$ (such interpetations may still be called conditions) and express the solution to the problem as some suitable operation on them. In general, it may be necessary to find a *compactification* $\bar{\mathcal{M}}$ of $\mathcal{M}$ with some convenient properties.

- *Effective computations*: In general, getting the value of the expressions may be achieved by a computer program capable of encoding the formalism.

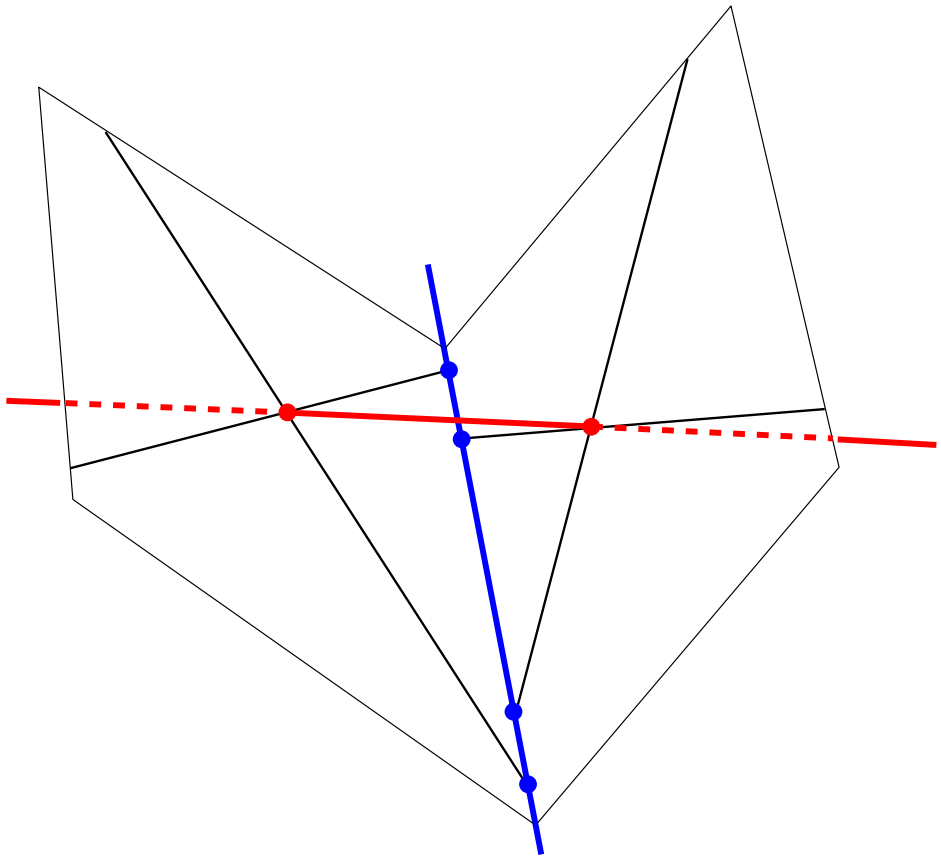
Remark: The calculus of conditions may be some existing calculus on some kind of spaces that has interest by itself, regardless of the enumerative problems to which it may be applied. To a large extend, this is the way we will follow here. This will include constructs and results of what is loosely called *intersection theory* on smooth algebraic varieties, but we will also be looking at examples that require other frameworks.

It is healthy to be aware, nevertheless, that historically the unfolding of intersection theory, or of algebraic geometry in general, has often been driven by the demands of particular enumerative problems, and that there has been a very broad interaction of these ideas with those of other areas, like mathematical logic (ever since Boole), or topology (ever since Poincaré), or differential geometry (ever since E. Cartan, and G. de Rham). In the latter two cases, the 'calculus of conditions' is some suitable cohomology ring.

On the other hand, once we have a calculus of conditions, there still remain the questions about how to apply it to concrete problems and, beyond that, about how to implement it in a computer system, which in our view has its own independent interest –for its own sake, to be sure, but also for the inspiration it can afford for other endeavors.

- *How many lines meet 4 given lines in* $\mathbf{P}^3$*?*

Poncelet's argument. By the 'principle of continuity', the problem is reduced to the case in which the first and second lines meet, and the same with the third and fourth. Then there are two lines solving the problem, as depicted in the figure.



Analytical solution. The lines meeting three lines swap a quadric: impose the condition that the line through a point x that meets the first two lines also meets the third. Now a forth line meets this quadric in two points, to which there correspond two lines meeting the four given lines.

Plücker-Klein solution. The lines in $\mathbf{P}^3$ form, through the Plücker embedding,[1] a quadric Q of $\mathbf{P}^5$ and the lines meeting a given line ℓ form the section of Q by the tangent hyperplane $T_\ell Q$. Therefore, the lines meeting the four given lines ℓ_1, ℓ_2, ℓ_3, ℓ_4 form the section of the line $T_{\ell_1} \cap T_{\ell_2} \cap T_{\ell_3} \cap T_{\ell_4}$ of $\mathbf{P}^5$ with Q, so the solution is 2.

[1] The Plücker coordinates $(p_{01}, p_{02}, p_{03}, p_{12}, p_{13}, p_{23})$ of the line ℓ joining the points $[x_0, x_1, x_2, x_3]$ and $[y_0, y_1, y_2, y_3]$ are given by the formula $p_{i,j} = x_i y_j - x_j y_i$. The vanishing of $\det(x, y, x, y)$ yields, using the Laplace rule, the quadratic relation $p_{01}p_{23} - p_{02}p_{13} + p_{03}p_{12} = 0$ (*Klein's quadric*).

Schubert calculus. Let l be the condition that a line meets a given line, p that it goes through a given point, and π that it lies in a given plane. Then $l^2 = \pi + p$ (as in Poncelet's argument, assume that the two line are coplanary). Since $p\pi = 0$, $l^4 = p^2 + \pi^2$ and hence the solution is 2: there is a unique line joining two points and a unique line lying in two planes.

Hilbert's 15: *To put Schubert's enumerative calculus on a rigorous foundation*.

Apollonius problem

Preliminary overview. Cartesian approach. Solution by Lie's circle geometry. Generalizations and related systems.

Apollonius problem

- *How many circles are tangent to 3 given circles?*

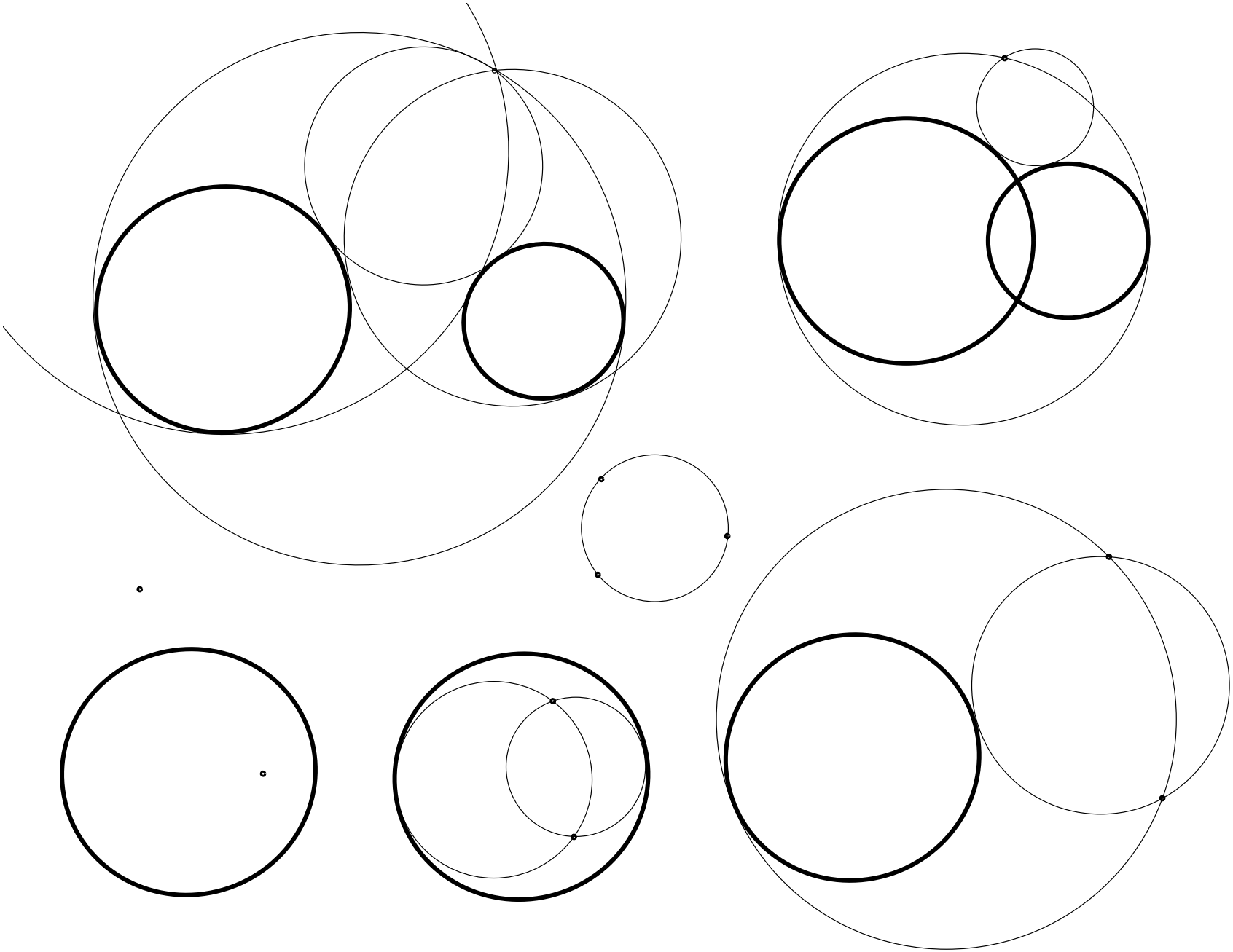
Special cases

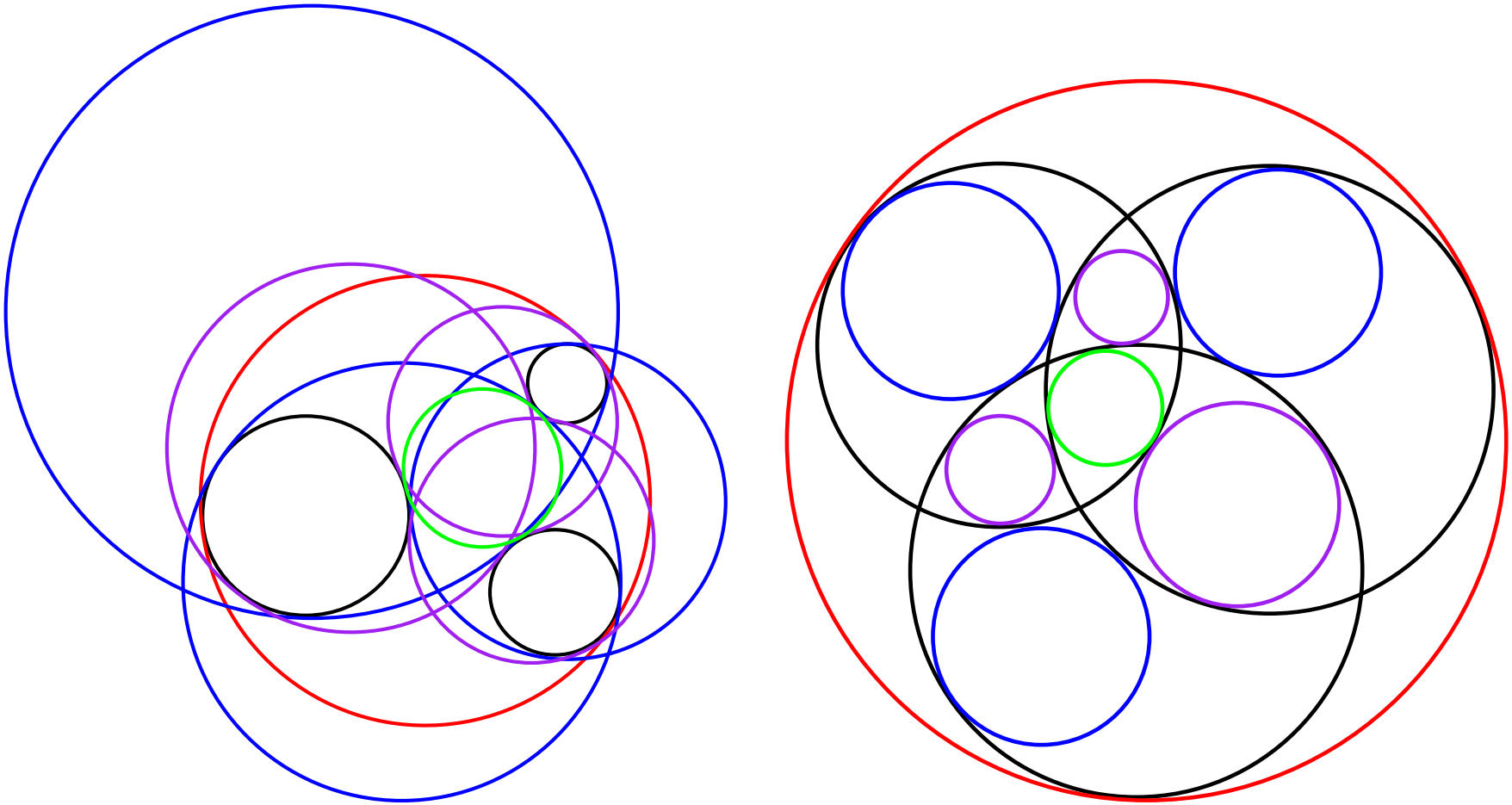
1) *How many circles going through one given point are tangent to two given circles?*

2) *How many circles going through two given points are tangent to one given circle?*

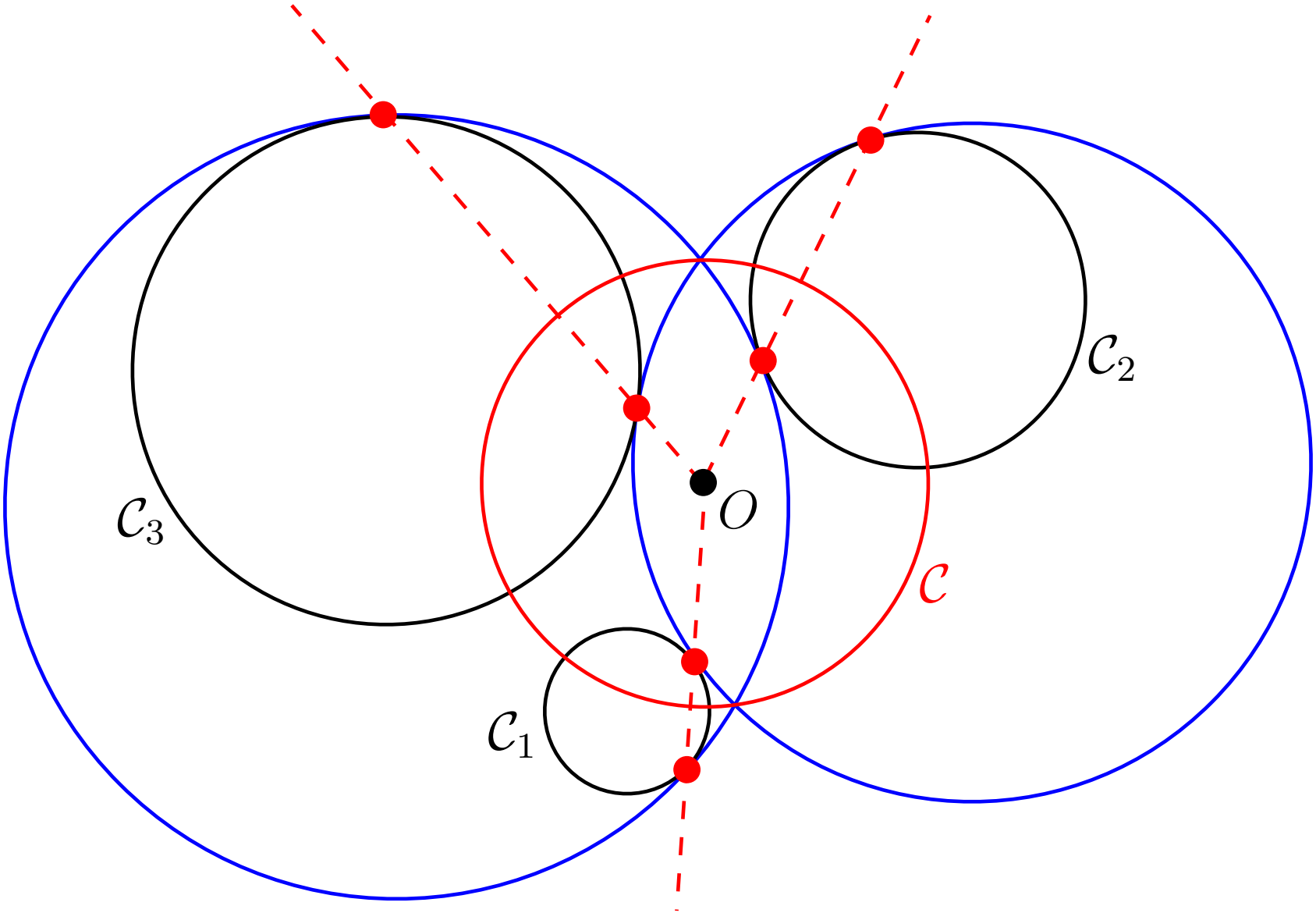
3) *How many circles pass through three given points?*

The solutions: (3) one, known since Euclid; (2) Known by Apollonius: two if the points lie on the same side of the circle, none otherwise; (1) the inversion with center at the point shows that there are as many as common tangent lines to two circles, which is 4 if the circles are disjoint or lower according to the relative position of the circles.



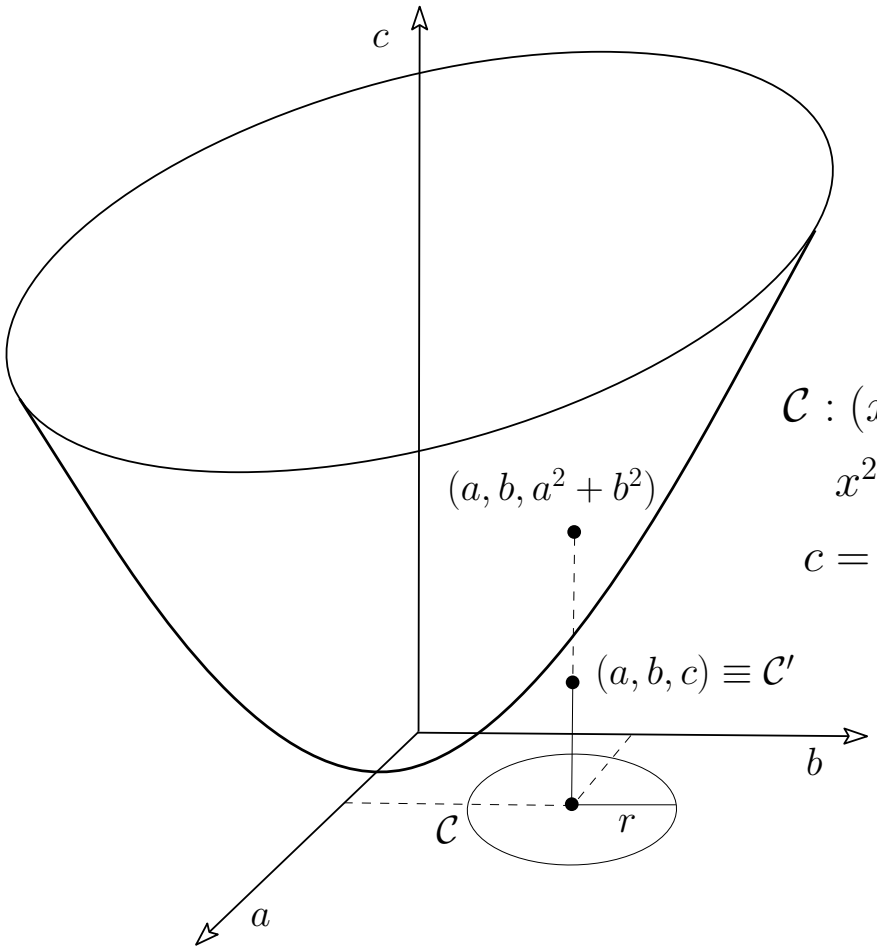


The three given circles are drawn in black. On the left, they are totally disjoint, and on the right they overlap but no one is contained in another. In both cases we see eight solutions to the problem: four pairs of 'conjugate' solutions (in the sense of next slide).



O ($\mathcal{C}$): radical center (circle) of $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$

Moduli. We can take the open set of $\mathbf{R}^3$ formed by the points (a, b, c) such that $a^2 + b^2 - c > 0$, as suggested by the equation $f_{a,b,c}(x, y) = x^2 + y^2 - 2ax - 2by + c = 0$ for the circle with center at (a, b) and radius $r = \sqrt{a^2 + b^2 - c}$.



$$\mathcal{C} : (x-a)^2 + (y-b)^2 = r^2$$
$$x^2 + y^2 - 2ax - 2by + c$$
$$c = a^2 + b^2 - r^2 < a^2 + b^2$$

Another view of the geometric discussion on pages 32-34.

Conditions. That the circle $f_{a,b,c} = 0$ goes through the point (x_0, y_0) is represented by the *abc*-plane $2x_0a + 2y_0b = c + x_0^2 + y_0^2$. This implies that *through three non collinear points there goes a unique circle*.

The intersection of $f_{a,b,c} = 0$ with the line $y = px + q$ is obtained by solving the quadratic equation $f_{a,b,c}(x, px + q) = 0$, so the condition for the circle to be tangent to the line is the vanishing of the discriminant, which turns out to be a quadratic equation in a, b, c, namely $(a + pb - pq)^2 - (1 + p^2)(c + q^2 - 2qb) = 0$ (if the line is vertical, say $x = k$, the condition is $b^2 - 2ka + c - k^2 = 0$). This implies that the condition for $f_{a,b,c}$ to be tangent to a given circle is also quadratic in a, b, c, as it is equivalent to the tangency to the radical axis of the two circles $(2(a - a')x + 2(b - b')y = c - c')$.

Calculus of conditions. Let us note that there are *two circles that go through two given points that are tangent to one given circle* (intersection of a quadric with a line), and that there are *four circles that go through one point and are tangent to two given circles* (common points of a plane with two quadrics, which amounts to the intersection of two conics in one plane).

As we will see later (Bézout's theorem for $\mathbf{P}^3$), the intersection of three quadrics has, if finite, at most 2^3 points, which is exactly 8 if we take into account complex solutions and each to them is counted with a suitable multiplicity. By what we saw before, in general the solutions are real and have multiplicity 1.

This is a nice example for the illustration of the general ideas presented on pages 23-24.

A very useful reference for our purposes has been the book *Geometriekalküle* of Jürgen Richter-Gebert and Thorsten Orendt (Springer, 2009), particularly Ch. 10 (*Kreisgeometrie*).

The *Lie vector* of the circle with center $M = (a, b)$ (*midpoint*) and radius R is the 5-vector

$$[w, 1 - w, a, b, R], \quad w = (1 + a^2 + b^2 - R^2)/2.$$

In particular, points are encoded as circles of radius 0.

Comparing with the Cartesian equation:

$$(x - a)^2 + (y - b)^2 = R^2, \quad \text{or}$$

$$x^2 + y^2 - 2ax - 2by + c, \quad c = a^2 + b^2 - R^2,$$

we see that $w = (1 + c)/2$, $1 - w = (1 - c)/2$.

For nonzero R, the *orientation* of the circle is encoded as the sign of R, a convention that is consistent with the customary parametric representation of the circle:

$$(x, y) = (a + R\cos(t), b + R\sin(t)), \quad t \in [0, 2\pi).$$

The *Lie vector of the line* $ax + by = d$, where (a, b) is its normal vector and $d = au + bv$ for any given point on it, is the 5-vector

$$\left[d, -d, a, b, \sqrt{a^2 + b^2}\right].$$

Lines can be considered as circles of radius ∞. In fact, it is a straightforward exercise to show that the Lie vector of the circle through the point $R = (u, v)$ with center at the point $M = (u + ta, v + tb)$ becomes, when $r \to \infty$, the Lie vector of the line through R with normal vector (a, b).

```
def Lie_vector(M=(0,0),R=0):
    a, b = M
    if is_pair(R):
        u,v = R
        d = a*u+b*v
        return [d,-d,a,b,sqrt(a**2+b**2)]
    if is_real(R):
        w = (1+a**2+b**2-R**2)/2
        return [w,1-w,a,b,R]
    return 'Lie_vector: wrong parameters'
LV = lie_vector=Lie_vector

def orientation(X):
    r = X[4]
    if r>0: return 1
    elif r<0: return -1
    else: return "orientation: object has no orientation"
```

The Lie metric. It is defined on 5-vectors by the formula

$$L(X,Y) = -x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 - x_5y_5.$$

Thus its signature is $(-,+,+,+,-)$.

In the implementations, we add a definition for 4-vectors identified with the 5-vectors whose last component is 0.

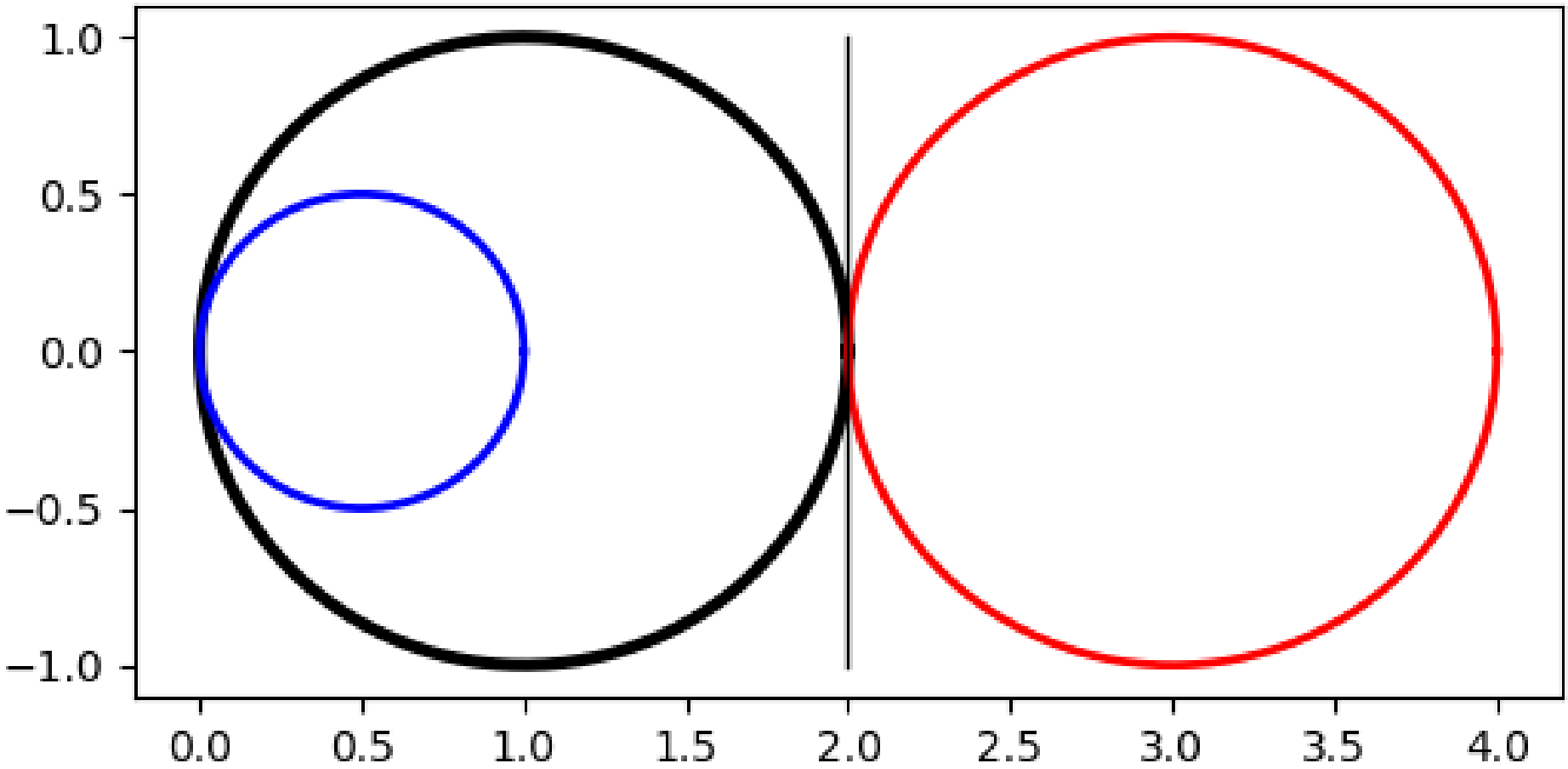
```
def Lie_metric(X,Y):
    if len(X)==len(Y)==4: # make them 5-vectors
        X[4] = Y[4] = 0
    x1,x2,x3,x4,x5 = X
    y1,y2,y3,y4,y5 = Y
    lm = -x1*y1 + x2*y2 + x3*y3 + x4*y4 - x5*y5
    if nil(lm): return 0
    return lm
#
LM = lie_metric = Lie_metric
```

Theorem. If X and Y are Lie vectors, the relation $L(X, Y) = 0$ is satisfied if and only if the corresponding circles have an oriented contact.

Remarks. Two distinct circles that touch intersect at a single point. The contact is internal (external) if they have the same (distinct) orientation.

If one of the circles is a line, the distinction is whether the normal vector to the line is pointing outwards or inwards of the circle.

If X is a point, the notion of oriented contact just means that the circle or line corresponding to Y goes through the point corresponding to X. If in addition Y is a point, it means that the points coincide.



If the three circles are positively oriented (counterclockwise by convention) and the line orientation is upwards, the oriented contacts occur for the blue and black circles and for the black circle and the line. The contacts of the red circle with the black circle and the line are not oriented contacts.

Lie quadratic form

It is the quadratic form of the Lie metric. It defines a non-degenerate quadric $\bar{\mathcal{C}}$ in $\mathbf{P}^4$. The points of this quadric are precisely those represented by the Lie vectors of circles, lines and points of the plane, together with the point $\infty = [1, -1, 0, 0, 0]$. In other words, it is a compactification of the space $\mathcal{C}$ of oriented circles in the Euclidean plain obtained by adding points (as circles of radius 0) and lines (as circles of radius ∞ or, equivalently, circles going through ∞).

```
def Lie_form(X): return Lie_metric(X,X)
```

Lie-Gram matrix

```
def lie_gram_matrix(*S):
    M = [[Lie_metric(X,Y) for X in S] for Y in S]
    return M
```

Cutting the Lie quadric with a line

Given three linearly independent 5-vectors A, B, C, which may or may not belong to the Lie quadric, the next function finds the (normalized) intersections with the Lie isotropic cone of the plane Lie-orthogonal to $\langle A, B, C\rangle$. This amounts to cut the Lie quadric with the line represented by $\langle A, B, C\rangle^{\perp_L}$.

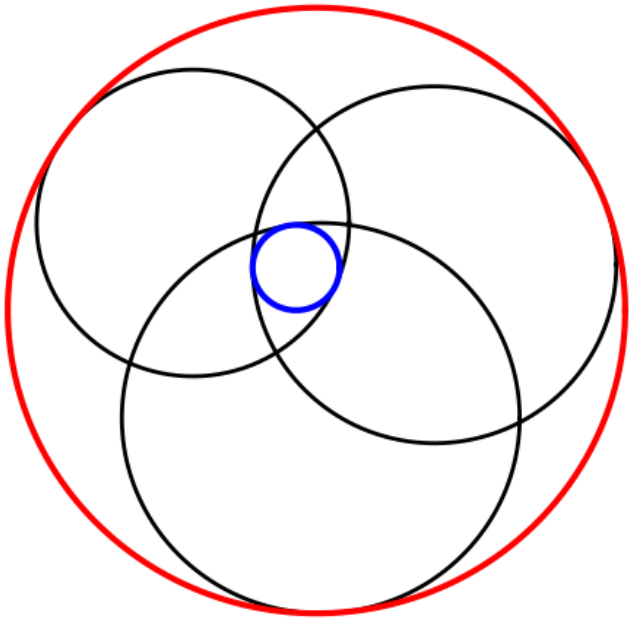
```
def Lie_section(A,B,C):
    X = A[:]; X[0]=-X[0]; X[4]=-X[4]
    Y = B[:]; Y[0]=-Y[0]; Y[4]=-Y[4]
    Z = C[:]; Z[0]=-Z[0]; Z[4]=-Z[4]
    import sympy
    M = sympy.Matrix([X,Y,Z])
    K = M.nullspace()
    if len(K)>2: return 'lie_section: Infinite solutions'
    else: [v,w] = K
    G = lie_gram_matrix(v,w)
    st = solve_quadratic(G[0][0],2*G[0][1],G[1][1])
    if st==0:
        print('lie_section: imaginary Lie objects')
        return 0
    s,t = st
    s1,s2 = s; t1,t2=t
    S = list(s1*v + s2*w); T = list(t1*v + t2*w)
    return normalize(S), normalize(T)
```

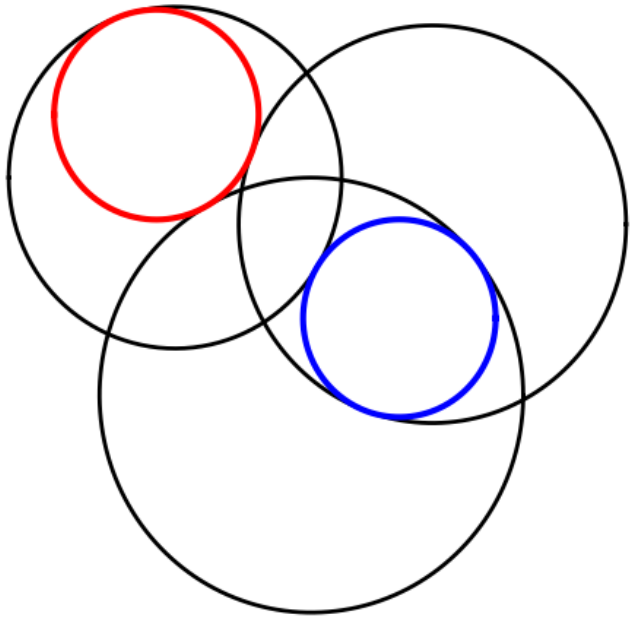
Examples

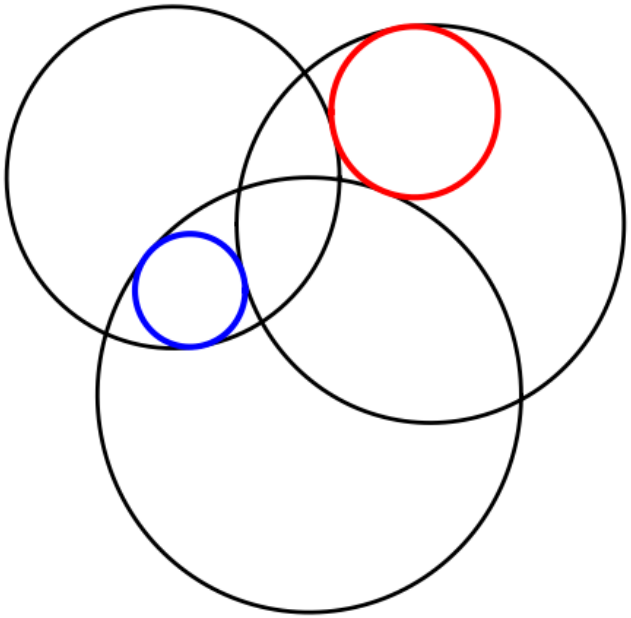
There are two circles (possibly imaginary) that properly touch three given circles X, Y, Z. These circles are delivered by Lie_section(X,Y,Z) and we may denote them by the expression $\circ\circ(X, Y, Z)$.

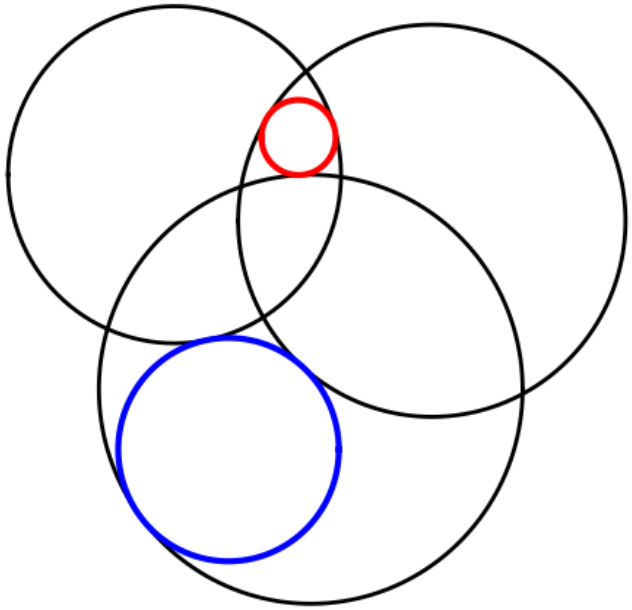
Changing the orientations of X, Y, Z simultaneously, $(\bar{X}, \bar{Y}, \bar{Z})$ yields the same pair of circles, but with exchanged roles with respect to the kind of oriented tangency.

It follows that we get four pairs of circles touchig the three given ones: $\circ\circ(X, Y, Z)$, $\circ\circ(X, Y, \bar{Z})$, $\circ\circ(X, \bar{Y}, Z)$, and $\circ\circ(X, \bar{Y}, \bar{Z})$.









The Apollonius problem and its effective solutions have occupied the minds of many prominent mathematicians since Apollonius contributions.

- General survey: [31] (Wikipedia)
- [16, Ch. 10, *Kreisgeometrie*] (RichterGebert-Orendt-2009, *Geometriekalküle*)
- [4, §III.2] (Courant-Robbins-1996, *What is Mathematics?*)
- [1] (Behnke-et-al-1974, *Fundamentals of mathematics, II: Geometry*): An excellent pedagogical introduction to Lie circle geometry and subordinated geometries (notably Laguerre and Möbius geometries).
- [5] (Coxeter-Greitzer-1967, *Geometry revisited*)
- [15, Chapter IV] (Pedoe-1970, *Geometry, a comprehensive course*)

As it is to be expected, there have been many generalizations of the Apollonius problem, which often have interesting connections with other areas.

- [3] (Cecil-2008, *Lie Sphere Geometry. With Applications to Submanifolds*): A thourough treatment of Lie sphere geometry.
- [36] (Zlobec-Kosta-2001, *Configurations of circles and the Apollonius problem*): this paper frames the generalization of Apolonius problems for spheres in $\mathbf{R}^n$ and uses the formalism of Lie's geometry to interpret and solve them.
- [14, §2.7, Möbius geometry] (Onishchik-Sulanke-2006, *Projective and Cayley-Klein geometries*)

- [24] (Sulanke-2019, *Differential Geometry of the Möbius Space I*)
- [8] (HertrichJeromin-2003, *Introduction to Möbius Differential Geometry*)
- [9] (Kisil-2018, *Lectures on Moebius-Lie Geometry and its Extension*): "review the classical Möbius-Lie geometry and recent work on its extension". Interesting computational treatment in C++ and an "interactive Python wrapper".

- Lie sphere geometry is very closely connected with Conformal Geometric Algebra and Oriented CGA. See [Ch. 2][11] (Lavor-Xambo-Zaplana-2018, *A geometric algebre invitation to space-time physics, robotics and molecular geometry*) and [2] (Cameron-JLasenby-2008, *Oriented conformal geometric algebra*), respectively, and the references therein. For CGA, see also [34] (Xambo-2016, talk at IMUVA).
- The method used to parametrize circles in the plane and lines in $\mathbf{P}^3$ by means of the Lie quadric in $\mathbf{P}^4$ and the Klein quadric in $\mathbf{P}^5$, respectively, was applied by Study to parametrize Euclidean proper displacements (moduli of the positions of a rigid body) by points of a quadric in $\mathbf{P}^7$. This approach, combined with geometric algebra techniques, is widely used in robot kinematics.
- [13] (Mumford-Series-Wright-2002, *Indra's pearls*)

.

1. **PyM structure. Examples.**

2. **Work on** `wit_lie`. Work out some the solution for three specific non-overlapping circles. Similarly, when one or more circles are lines or points.

Plane curves

Geometric features and numerical charaters. Tangents. Intersection multiplicity and Fulton's algorithm. Polars, dual curve and Plücker formulas. Bézout's theorem and the resultant. Rational plane curves and Kontsevich numbers.

- *Plane curves*: Let $\bar{C} = Z(F) \subset \mathbf{P}^2$ be a (projective) plane curve, where $F \in K[x_0, x_1, x_2] - \{0\}$ is homogeneous. Unless declared otherwise, K is an algebraically closed field of characteristic 0 (say $\mathbf{C}$).

- The polynomial $f = F(1, x, y) \in K[x, y]$ is the *dehomogenization* of F (with respect to x_0). If F is not divisible by x_0, we have $F = x_0^d f(x_1/x_0, x_2/x_0)$, which is the *homogenization* of f. Explicitly, if $f = f_0(x, y) + f_1(x, y) + \cdots + f_d(x, y)$, where f_j is the homogeneous component of degree j of f, then $F = x_0^d f_0 + x_0^{d-1} f_1 + \cdots + x_0 f_{d-1} + f_d$.

- In practice, we can deal with $\bar{C}$ by means of $C = Z(f) \subset \mathbf{A}^2$ (*affine curve*) for *proper* points together with the analysis of the *improper* points of $\bar{C}$, namely $Z(f_d(x_1, x_2), x_0)$.

- *Components*: If $F = F_1^{r_1} \cdots F_m^{r_m}$ is the factorization of F into irreducible homogeneous polynomials $F_1, \ldots, F_m$, $\bar{C}_i = Z(F_i)$ are the irreducible *components* of $\bar{C}$ and $r_1, \ldots, r_m$ are their multiplicities.

- *Degree d*: Algebraically, the total degree of F; geometrically, the maximum number of intersection points of C with a line L (count points on $C_i \cap L$ with multiplicity r_i). Curves of degree $d = 2, 3, 4, 5, \ldots$ are called *conics*, *cubics*, *quartics*, *quintics*, ...

- *Moduli*: $\mathbf{P}^{N_d}$, $N_d = (d+2)(d+1)/2 - 1 = d(d+3)/2$.

- *Remark*: The above definitions are valid for any number of variables $x_0, x_1, \ldots, x_n$, except that for $n > 2$ the locus $Z(F)$ is called a *hypersurface* and 'conic' is replaced by *quadric* for $n \geqslant 3$ and (often) by *hyperquadric* for $n > 3$. The moduli space is $\mathbf{P}^{N_{n,d}}$, $N_{n,d} = \binom{n+d}{d} - 1$.

Note also that the condition of passing through a point is linear.

- The case $n = 1$ is special: The irreducible factors of F can be written in the form $F_i = b_i x_0 - a_i x_1$ and hence $\bar{C}_i = Z(F_i)$ is the point $[a_i, b_i] \in \mathbf{P}^1$, which is $[1, b_i/a_i]$ if $a_i \neq 0$ and $\infty = [0, 1]$ if $a_i = 0$.

Thus $Z(F)$ has d points (when counted with their multiplicities r_i). These points are all proper if x_0 is not a factor of F; otherwise, ∞ appears with the multiplicity of x_0 as a factor of F.

- This result was used by Poncelet to justify what he called the *principle of continuity* and later (Severi, [23]) the principle of *conservation of number*. See [32] for a historical overview.

- *Multiplicity* of point O on C, $m = m_O(C)$: The maximum m such that all partial derivatives of F of order $< m$ vanish at O. We see that $m_O(C)$ is 0 for any point O not on C and $m_O(C) \geqslant 1$ for all $O \in C$.

- $m_O(C)$ is also the minimum of $i_O(C, L)$ for L a line through O. Note that the points $O \in C \cap L$ correspond to the roots of the restriction of F to L, and $i_O(C, L)$ is the multiplicity of the root corresponding to O. The sum of these multiplicities is d, and they are all equal to 1 for generic L if the curve is *reduced* (i.e., has no multiple factors).

- A point $O \in C$ is *simple* or *smooth* (*multiple* or *singular*) if $m = 1$ ($m > 1$). For $m = 2$, $m = 3$ and $m = 4$ we say *double*, *triple* and *quadruple* points, respectively.

- *Tangents*: The tangents to C at O are the lines given by the linear factors of $f_m(x, y)$, where $f(x, y) = f_m(x, y) + \cdots + f_d(x, y)$ is the equation of C in affine coordinates x, y with origin at O. Each tangent has a multiplicity and the sum of these multiplicities is m. A multiple point ($m > 1$) is *ordinary* if its tangents have multiplicity 1, i.e., if they are all distinct.

- A *node* (*cusp*) is a double point with two distinct (coincident) tangents. The origin is a cusp, with double tangent $y = 0$, for $y^2 - x^3 = 0$ and a node, with tangents $y \pm x = 0$, for $y^2 = x^2 + x^3$.

- *Intersection multiplicity* of C and C' at a point O, $i_O(C, C')$: $\dim \mathcal{O}_{\mathbf{P},O}(f, g)$, the dimension of the quotient of the local ring of the plane at O by the ideal generated by the local equations f and g of C and C' at O.

We will also write $i_O(F, F')$ instead of $i_O(C, C')$).

- If $O = [a, b, 1] = (a, b)$ is a proper point (i.e. a point in $\mathbf{A}^2 = \mathbf{P}^2 - \{Z = 0\}$, $i_O(F, F')$ only depends on $f(x, y) = F(x, y, 1)$, $g(x, y) = G(x, y, 1)$ and (a, b), and is denoted $i_O(f, g) = i_{(a,b)}(f, g)$.
- If $O = [a, 1, 0]$, then $i_O(F, G) = i_{(a,0)}(F(x, 1, z), G(x, 1, z))$, and if $O = [1, 0, 0]$, then $i_O(F, G) = i_{(0,0)}(F(1, y, z), G(1, y, z))$.
- Since $i_{(a,b)}(f, g) = i_{(0,0)}(f(x + a, y + b), g(x + a, y + b))$, we can assume that $a = b = 0$, i.e. $O = (0, 0)$.
- $i_P(C, C') \geqslant e_P(C)e_P(C')$, $=$ if and only if C and C' do not have common tangents at P. In particular $i_P(C, C') = 1$ if and only if P is a smooth point on both C and C' and C and C' are not tangent at P.
- Bézout's theorem: If C and C' have degrees d and d' and no common component, then the number of intersection points of C and C', counted with their intersection multiplicities, is dd'. See [30, §5.2] (Waker-1950, *Algebraic curves*).

The function imult(f, g) computes the intersection multiplicity of the plane curves $f(x, y) = 0$ and $g(x, y) = 0$ at the point $O = [a, b]$, which by default is taken to be the origin $O = [0, 0]$. The algoritm is extracted from Fulton's book *Algebraic Curves* (see `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`, Section 3.3). Two instances of Fulton's example (*loc. cit.*, page 40):

```
F = Q_       # in this case it yields 14
# F = Zn(5) # in this case it yields 18

[Fxy,x,y] = polynomial_ring(F,'x','y','Fxy')

f = (x**2 + y**2)**3 - 4*x**2 * y**2
g = (x**2 + y**2)**2 + 3*x**2 * y - y**3

show(imult(f,g))
```

The algorith works as follows. We may assume $f \neq 0$ and $g \neq 0$, as otherwise the $i(f,g) = \infty$. Write

$$f = f_0 + f_1 y + \cdots + f_m y^m, \quad g = g_0 + g_1 y + \cdots + g_n y^n, \quad f_m, g_n \neq 0.$$

If $f_0 = 0$, then $f = f'y$, $f' = f_1 + \cdots + f_m y^{m-1}$, and hence $i(f,g) = i(f'y,g) = i(y,g) + i(f',g) = i(y,g_0) + i(f',g)$. We can assume that $g_0 \neq 0$, as otherwise $i(y,g_0) = \infty$, and then $i(y,g_0)$ is equal to the *trailing degree* of g_0, that is, the degree of the lowest non-zero monomial appearing in g_0, which is positive, and so we can proceed recursively with $i(f',g)$. If $g_0 = 0$, we can proceed likewise. Thus we can assume that $f_0, g_0 \neq 0$. Let r, s be the degrees of these polynomials, and assume $r \geqslant s$ (this is no loss of generality). If c_0, d_0 are the leading coefficients of f_0 and g_0, respectively, then $i(f,g) = i(d_0 f - c_0 x^{r-s} g, g)$, which reduces the problem to a case with lower r and same s, and so we can proceed recursively.

```
def imult(f,g,O=[0,0]):
    if f==0 or g==0: return 'Infinity'
    if evaluate(f,[x,y],O)!= 0 or evaluate(g,[x,y],O)!=0: return 0
    a = O[0]; b = O[1]
    if a!=0 or b!=0:
        f = evaluate(f,[x,y],[x+a,y+b])
        g = evaluate(g,[x,y],[x+a,y+b])
    f0 = constant_coeff(f); r = degree(f0)
    g0 = constant_coeff(g); s = degree(g0)
    if f0==0:
        if g0==0: return 'Infinity'
        else: return trailing_degree(g0) + imult(f/y,g)
    else: # f0!=0
        if g0==0: return trailing_degree(f0)+imult(f,g/y)
        else: # g0!=0
            c0 = leading_coeff(f0); d0 = leading_coeff(g0)
            if r<=s: return imult(f,c0*g-d0*x**(s-r)*f)
            else: return imult(d0*f-c0*x**(r-s)*g,g)
    return 'Error'
```

- *Conjugate points*. Let $C = Z(F)$. Given points $X = [x_0, x_1, x_2] = [x]$ and $Y = [y_0, y_1, y_2] = [y]$, we say that they are *conjugate* with respect to C if

$$y \cdot \boldsymbol{\partial} F(x) = y_0 \partial_0 F(x) + y_1 \partial_1 F(x) + y_2 \partial_2 F(x) = 0.$$

If we fix $X \in C$, then the conjugate points of X are those of the tangent line $T_X C$ to C at X, if X is smooth, and all points of the plane otherwise.

- *Polar curves*. If we fix Y, then the points X conjugate to Y form the curve $C_Y = Z(y_0 \partial_0 F(x) + y_1 \partial_1 F(x) + y_2 \partial_2 F(x))$, which is called the (first) *polar* of Y with respect to C. This curve has degree $d - 1$, passes through all singular points of C, and if $X \in C \cap C_Y$ is smooth on C, then Y lies on $T_X C$.

- *Dual curve*. If C is irreducible of degree $d > 1$, the set of tangents at smooth points of C is an open set of an irreducible curve in $\mathbf{P}^\vee$. This curve is called the *dual* curve of C and is denoted $C^\vee$. The degree of $C^\vee$, denoted $d^\vee$, is also called the *class* of C. Thus $d^\vee$ is the number of proper tangents of C passing through a general point of $\mathbf{P}$.

- *Plücker's class formula*. Let C be an irreducible plane curve of degree d and class $d^\vee$. Assume that the only singularities of C are δ ordinary nodes and κ ordinary cusps. Then *Plücker's formula* for the class is the following:

$$d^\vee = d(d-1) - 2\delta - 3\kappa\ . \tag{1}$$

In other words, a node counts with multiplicity 2 in the intersection of C and C_P, and a cusp with multiplicity 3.

Expression of d^v in terms of the genus. Let g be the geometric genus of a curve C. If C satisfies the same hypothesis as in the preceding paragraph, then, as proved by Clebsch in 1864,

$$g = \frac{(d-1)(d-2)}{2} - (\delta + \kappa) \; . \tag{2}$$

This formula, and Plücker's first formula, imply that

$$d^v = 2d + (2g-2) - \kappa \; . \tag{3}$$

- *Plücker's dual formula*. The nodes of $C^{\vee}$ are the *bitangent lines* of C, that is, the lines that are simply tangent to C at exactly two smooth points, and the cusps of $C^{\vee}$ are the inflexional tangents of C, that is, lines that are doubly tangent to C at one point (such point is called a *flex* of C) and that are transversal to C elsewhere.

Now it turns out that C is the dual of $C^{\vee}$ (this is the so called *biduality theorem*; for a nice proof see [10] (Kleiman-1977, *The enumerative theory of singularities*). So if the only multiple tangents of C are $\delta^{\vee}$ bitangent lines and $\kappa^{\vee}$ inflexional tangents, then

$$d = d^{\vee}(d^{\vee} - 1) - 2\delta^{\vee} - 3\kappa^{\vee} \,. \tag{4}$$

Furthermore, since C and $C^{\vee}$ have the same genus, for C and $C^{\vee}$ are birationally equivalent, we get that

$$d = 2d^{\vee} + (2g - 2) - \kappa^{\vee} \,. \tag{5}$$

- *Other Plücker formulas*: Eliminating g and $d^\vee$ between (7), (5) and (4), one obtains

$$k^\vee = 3d(d-2) - 6\delta - 8\kappa \ .$$

Dually,

$$k = 3d^\vee(d^\vee - 2) - 6\delta^\vee - 8\kappa^\vee \ .$$

Similarly one obtains that

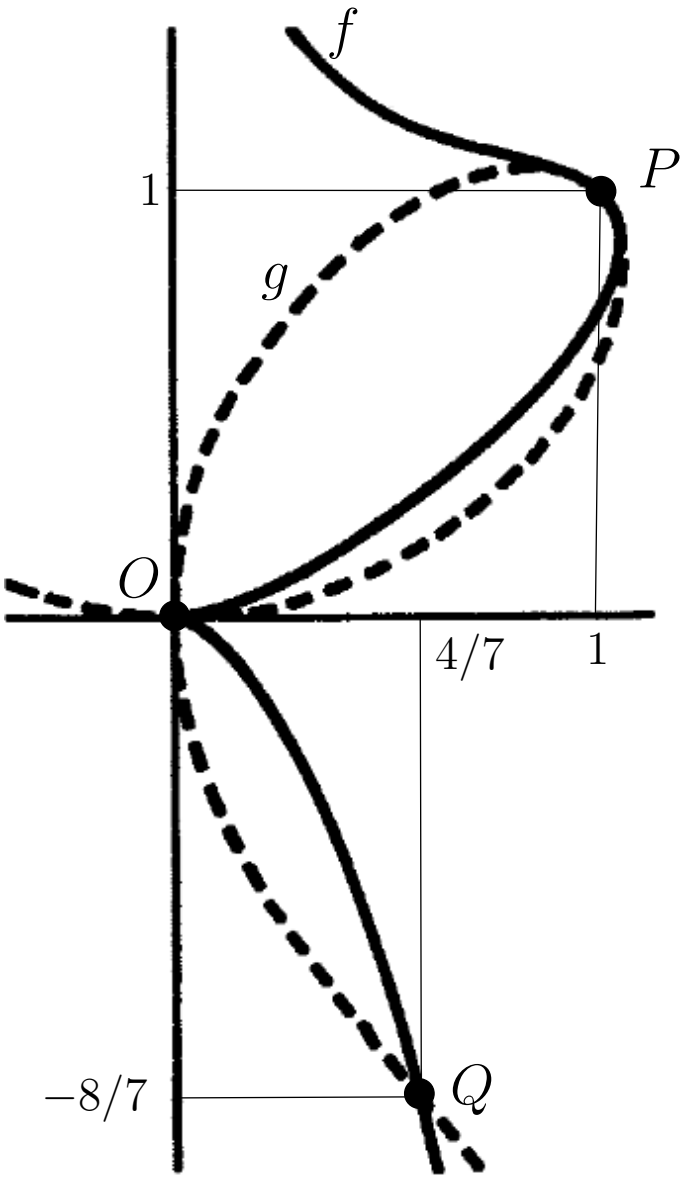
$$\delta^\vee = \frac{d(d-2)(d^2-9)}{2} \ .$$

Hence a smooth quartic has 28 bitangent lines.

If the base field is algebraically closed, two reduced plane curves of degrees m and n with no common components have exactly mn intersection points provided that the points at infinity are taken into account and that each point is counted with its intersection multiplicity.

In the classical theory, the standard proof of Bézout's theorem relies on the properties of the resultant $R = R_y(f, g)$ of the curves, which include a definition of the intersection multiplicities at the common points. Van der Waerden's book [27] features the first presentation using the algebraic methods developed by the E. Nother's school that crystallized in [28]. For an historical account, see for instance [29]. Nowadays, the best treatment is provided in [6, Ch. 1]: Examples 1.1.1, 1.2.1, 1.2.5 and 1.4.1 address, respectively, the definition and properties of $i_P(f, g)$; the relation of the resultant with the intersection multiplicities; Zeuthen's rule (see also [30, IV,§5]); and a proof of Bézout's theorem that vindicates Poncelet's approach.

Example



This figure is adapted from Fig 5.1 on page 112 of Walker's book *Algeraic curves*. It depicts two cubics, f and g, having a cusp and a node at O, respectively:

$$f = x^3 + y^3 - 2xy, \quad g = 2x^3 - 4x^2y + 3xy^2 + y^3 - 2y^2.$$

The `imult` algorithm gives $i_O(f, g) = 5$. Besides O, it is immediate that the point $P(1, 1)$ also lies on f and g, and we find that $i_P(f, g) = 3$. By Bzout's theorem, there must be another intersection point with multiplicity 1. This point can be found with the resultant $R = R(f, g)$, which is, up to a cancelled factor $8x^5(x-1)^3$, $-4 + 7x$, which vanishes at $x_0 = 4/7$. It follows that the polynomials $f(x_0, y)$ and $g(x_0, y)$ have a common root. Now their difference is a quadratic polynomial whose roots turn out to be $-8/7$ and $4/7$. Then if we set $Q = (4/7, -8/7)$ and $Q' = (4/7, 4/7)$, we get $i_Q(f, g) = 1$ and $i_{Q'}(f, g) = 0$. Therefore the intersection of the two curves is $5O + 3P + Q$. Note that the values of f and g at Q', which are nonzero, must be the same because their difference vanishes at Q'.

Consider the set (variety) of plane *rational* curves of degree d. If we consider curves with no other singularities than δ nodes, we get a variety $V_{d,\delta}$ of dimension $d(d+3)/2-\delta$. If we want rational curves ($g=0$), than $\delta=(d-1)(d-2)/2$ and hence $R_d=V_{d,(d-1)(d-2)/2}$ has dimension $d(d+3)/2-(d-1)(d-2)/2=3d-1$.

Let N_d be the number of curves in R_d that pass through $3d-1$ points in general position.

- $N_1=1$: one line going through 2 distinct points.
- $N_2=1$: one conic going through 5 points if no four of them are collinear.

- $N_3 = 12$: number of nodal cubics going through 8 points (Steiner 1848 & 1853, Maillard 1871, Zeuthen 1872).
- $N_4 = 620$: number of rational quartics (3 nodes) going through 11 points (Zeuthen 1873).
- $N_5 = 87304$: number of rational quintics (6 nodes) going through 14 points (Ran 1989, Vainsencher 1995).

Theorem (Kontsevich 1995). Given $d \geqslant 2$, for each $j \in [1, d-1]$ let $k = d - j$. Then N_d satisfies the recursive relation

$$N_d + \sum_j \binom{3d-4}{3j-1} j^2 N_j N_k jk = \binom{3d-4}{3j-2} j N_j k N_k jk.$$

Since $N_1 = 1$, the relation allows us to compute N_d for all $d > 1$: setting $n = 3d - 4$ and $m = 3j - 2$, and using $\binom{n}{m+1} = \binom{n}{m}\frac{n-m}{m+1}$, we have

$$N_d = \sum_j j^2 k N_j N_k \binom{n}{m} \left(k - j\tfrac{n-m}{m+1}\right).$$

d	1	2	3	4	5	6	7
N_d	1	1	12	620	87304	26312976	14616808192

Remark: N_{100} has 520 digits and N_{200}, 1227.

```
## Number of rational plane curves of degree d >= 1
## going through 3d-1 points in general position

def K_(d):
    L = [1]
    for j in range(1,d):
        L = update(L)
    return L

def update(L):
    d = len(L)+1
    K = 0
    for j in range(1,d):
        k = d-j
        n = 3*d-4; m = 3*j-2
        B = binom(n,m)
        K += j**2 * k * L[j-1] * L[k-1] * ( B*k - j*B*(n-m)//(m+1)
    return L + [K]
```

Counting rational points on curves/F_q

The zeta function. Basic algorithm. Improved algorithm. The function XN. Elliptic curves over F_2. The Klein quartic.

We will follow [12] (Molina-Sayols-Xambo-2017, and references therein). Here X denotes a (smooth absolutely irreducible) curve/ F_q, and $g = g(X)$ its genus. The aim of this part is to explain an implementarion of a fast algorithm that finds, for any given r, the number ν_r of F_{q^r}-rational points on X assuming $\nu_1, \ldots, \nu_g$ are known.

Ingredients

- *The Hasse-Weil-Serre upper bound*. $\mathcal{N}_q(g) = q + 1 + g\lfloor 2\sqrt{q} \rfloor$ (upper bound for the number of F_q-rational points of X/F_q): [19] (Serre-1983), [20] (Serre-1983), [21] (Serre-1984).

For historical aspects and background: [25] (Torres-2008), [26] (van der Geer-2015), and the many references provided there. The general context provided by the Weil conjectures is outlined in [7] (Hartshorne, *Algebraic geometry*), Appendix C.

- $\nu_r = \nu_r(X)$ — $\#X(\mathbb{F}_{q^r})$
- $Z = Z(T) = \exp\left(\sum_{r=1}^{\infty} \nu_r \frac{T^r}{r}\right)$ — *Weil zeta function of X*

  $\nu_r = \frac{1}{(r-1)!}\frac{d^r}{dT^r} \log Z(T)|_{T=0}$.
- $Z(T) = \frac{P(T)}{(1-T)(1-qT)}$, $P(T) \in \mathbf{Z}[T]$ — *rationality*
- $P(T) = q^g T^{2g} P(1/qT)$ — *functional equation*

  $\deg(P) = 2g$
- $P(T) = \prod_{j=1}^{2g}(1-\alpha_j T)$, $|\alpha_j| = \sqrt{q}$ — *'Riemann hypothesis' for X*
- $\nu_r = q^r + 1 - S_r$, $S_r = \sum_{j=1}^{2g} \alpha_j^r$

Notations. $c_0 = 1$ and $c_j = (-1)^j \sigma_j(\alpha_1, \ldots, \alpha_{2g})$ for $j = 1, \ldots, 2g$.
Thus $P(T) = c_0 + c_1 T + \cdots + c_{2g} T^{2g}$ and $c_{2g} = q^g$.

Input: $\nu_1, \ldots, \nu_{2g}$ and $r > 2g$.

Output: $\nu_{2g+1}, \ldots, \nu_r$.

- For $j = 1, \ldots, 2g$, set $S_j = q^j + 1 - \nu_j$.
- Use the Girard-Newton formulas to recursively compute $c_1, \ldots, c_{2g}$:

$$c_j = -(S_j + c_1 S_{j-1} + \cdots + c_{j-1} S_1)/j.$$

- Use the Girard-Newton relation

$$S_j = -\left(c_1 S_{j-1} + \cdots + c_{2g-1} S_{j-(2g-1)} + c_{2g} S_{j-2g}\right)$$

to successively get S_j and $\nu_j = q^j + 1 - S_j$ for $j = 2g+1, \ldots, r$.

Proposition. $c_{g+l} = q^l c_{g-l}$.

Proof. If α_j is a root, $\bar{\alpha}_j = q/\alpha_j$ is a root (P has real coefficients). Possible real roots of P: $\pm\sqrt{q}$ (an even number). The multiplicity of $-\sqrt{q}$ is even (the coefficient of T^{2g} is q^g, by the functional equation). Index the roots of P so that $\alpha_{2g-j+1} = \bar{\alpha}_j = q/\alpha_j$, $j = 1, \ldots, g$. Now $\alpha_j \mapsto q/\alpha_j$ exchanges $\alpha_1, \ldots, \alpha_g$ and $\alpha_{2g}, \ldots, \alpha_{g+1}$. If we set

$$f(T) = \prod_{j=1}^{2g}(T - \alpha_j) = c_0 T^{2g} + c_1 T^{2g-1} + \cdots + c_{2g-1} T + c_{2g},$$

then $T^{2g} f(q/T)$ has the same roots as $f(T)$ and therefore $T^{2g} f(q/T) = c_{2g} f(T) = q^g f(T)$. Now the claim follows by equating the coefficients of T^{g+l} on both sides: on the right we get $q^g c_{g-l}$ and on the left $q^{g-l} c_{g+l}$. □

Input: $\nu_1, \ldots, \nu_g$ and $r > g$.

Output: $\nu_{g+1}, \ldots, \nu_r$.

- For $j = 1, \ldots, g$, set $S_j = q^j + 1 - \nu_j$.
- For $j = 1, \ldots, g$,
$$c_j = -(S_j + c_1 S_{j-1} + \cdots + c_{j-1} S_1)/j.$$
- For $j = g+1, \ldots, \min(r, 2g)$, set $c_j = q^{j-g} c_{2g-j}$, get
$$S_j = -(c_1 S_{j-1} + \cdots + c_{j-1} S_1 + j c_j),$$
and set $\nu_j = q^j + 1 - S_j$.
- If $r > 2g$, proceed as in the basic algorithm: for $j = 2g+1, \ldots, r$,
$$S_j = -(c_1 S_{j-1} + \cdots + c_{2g} S_{j-2g})$$
and set $\nu_j = q^j + 1 - S_j$.

The parameter X of the function XN denotes the list $[\nu_1, \ldots, \nu_g]$.

```
def XN(q,X,k):
    g = len(X)
    if k<=g: return X[:k]
    X = [0]+X           # trick so that X[j] refers to F_{q^j}
    X = [x>>Q_ for x in X]
    S = [q**(j)+1-X[j] for j in range(1,g+1)] # Newton sums
    S = [0]+S           # similar trick
    # Computation of c1,...,cg; set c0=1
    c = [1>>Q_]
    for j in range(1,g+1):
        cj = S[j]
        for i in range(1,j):
            cj += c[i]*S[j-i]
        c += [-cj/j]
```

```
#
# Add c_{g+i}, for i=1,...,g
for i in range(1,g+1):
    c += [q**i*c[g-i]]
# Find Sj for j = g+1,...,k
for j in range(g+1,k+1):
    if j>2*g:
        Sj=0
    else:
        Sj = j*c[j]
    for i in range(1,j):
        if i>2*g: break
        Sj += c[i]*S[j-i]
    S += [-Sj]
# Find X[i] for i = g+1,...,k
for i in range(g+1,k+1): X += [q**i+1-S[i]]
return vector(X[1:])
```

- $N_q(g)$: maximum of $\#X(\mathbb{F}_q)$ taken over all curves X of genus g. By the HWS upper bound,

$$N_q(g) \leqslant \mathcal{N}_q(g) = q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

- X of genus g is *maximal* if $\#X(\mathbb{F}_q) = N_q(g)$.
- *Deuring algorithm*: Yields the list of all possible $\#E(\mathbb{F}_q)$ for elliptic curves $E/\mathbb{F}_q$.

```
 q  m
 2  2 [1, 2, 3, 4, 5]
 3  3 [1, 2, 3, 4, 5, 6, 7]
 4  4 [1, 2, 3, 4, 5, 6, 7, 8, 9]
 5  4 [2, 3, 4, 5, 6, 7, 8, 9, 10]
 7  5 [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]
 8  5 [4, 5, 6, 8, 9, 10, 12, 13, 14]*
 9  6 [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]
11  6 [6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]
```

Missing values in the HWS range for elliptic curves. Here q is a prime power up to 5^3, $m = \lfloor 2\sqrt{q} \rfloor$ and d is the length of the Deuring list when less than $2m+1$.

q	2m+1	d	
8	11	9	[7, 11]
16	17	13	[11, 15, 19, 23]
25	21	20	[26]
27	21	17	[22, 25, 31, 34]
32	23	15	[23, 27, 29, 31, 35, 37, 39, 43]
49	29	27	[43, 57]
64	33	21	[51, 53, 55, 59, 61, 63, 67, 69, 71, 75, 77, 79]
81	37	29	[67, 70, 76, 79, 85, 88, 94, 97]
125	45	37	[106, 111, 116, 121, 131, 136, 141, 146]

Over $\mathbb{F}_2 = \mathbf{Z}_2$ there are 32 cubic polynomials in *normal form*

$$E = y^2 + a_1xy + a_3 + x^3 + a_2x^2 + a_4x + a_6$$

of which precisely 16 are non-singular. For these cases, $g = 1$, the HWS bound is $q + 1 + m = 5$ (as $m = \lfloor 2\sqrt{2} \rfloor = 2$) and we have seen that all the integers in the HWS interval $[1, 5]$ occur as $\nu_1(E)$ for some E. Now a straighforward computation yields the following distribution:

ν_1	E
1	$y^2+y+x^3+x+1,\ y^2+y+x^3+x^2+1$
2	$y^2+xy+x^3+x^2+1,\quad y^2+xy+x^3+x^2+x,$
	$y^2+(x+1)y+x^3+1,\quad y^2+(x+1)y+x^3+x+1$
3	$y^2+y+x^3,\quad y^2+y+x^3+1$
	$y^2+y+x^3+x^2+x,\quad y^2+y+x^3+x^2+x+1$
4	$y^2+xy+x^3+1,\quad y^2+xy+x^3+x$
	$y^2+(x+1)y+x^3+x^2,\quad y^2+(x+1)y+x^3+x^2+x$
5	$y^2+y+x^3+x,\quad y^2+y+x^3+x^2$

The sequences of values returned by XN with inputs $q=2$ and $[\nu_1]$, for $\nu_1=1,\ldots,5$, and $r=20$ are the following (the top row S is the maximum value $N_q(1)$ of $\#E(\mathbb{F}_q)$ supplied by "Serre's procedure":

r	1	2	3	4	5	6	7	8	9	10
$S(2^r)$	5	9	14	25	44	81	150	289	558	1089
ν_r	1	5	13	25	41	65	113	225	481	1025
	2	8	14	16	22	56	142	288	518	968
	3	9	9	9	33	81	129	225	513	1089
	4	8	4	16	44	56	116	288	508	968
	5	5	5	25	25	65	145	225	545	1025

r	11	12	13	14	15	16	17	18	19	20
S	2139	4225	8374	16641	33131	66049	131797	263169	525737	1050625
ν_r	2113	4225	8321	16385	32513	65025	130561	262145	525313	1050625
	1982	4144	8374	16472	32494	65088	131174	263144	525086	1047376
	2049	3969	8193	16641	32769	65025	131073	263169	524289	1046529
	2116	4144	8012	16472	33044	65088	130972	263144	523492	1047376
	1985	4225	8065	16385	33025	65025	131585	262145	523265	1050625

Remark. $\mathrm{XN}(q, [\nu_1, \ldots, \nu_g], \infty) = \{\nu_j(X/\mathbb{F}_q)\}_{j\geqslant 1}$. Given a positive integer s, the subsequence $\{\nu_{sj}(X/\mathbb{F}_q)\}_{j\geqslant 1}$ is $\{\nu_j(X/\mathbb{F}_{q^s})\}_{j\geqslant 1}$ and therefore it must agree with $\mathrm{XN}(q^s, [\nu_s, \ldots, \nu_{sg}], \infty)$.

Summary. The tables above show that the elliptic curves E_i $(i = 1, ..., 5)$ are maximal in 12 occasions over $\mathbb{F}_{2^r}$ in the range $r = 1, ..., 20$, and that they are close to the maximal value in the remaining cases:

- E_1 is maximal for $r = 4, 12, 20$, and is submaximal for $r = 19$.
- E_2 is maximal for $r = 3, 13$, and is submaximal for $r = 16$.
- E_3 is maximal for $r = 2, 6, 10, 14, 18$.
- E_4 is maximal for $r = 5$, and is submaximal for $r = 8, 11, 15, 16$ (the first and last tie with E_2).
- E_5 is maximal for $r = 1$, and is submaximal for $r = 7, 9, 16$.

The *Klein quartic* $C/\mathbb{F}_2$ ($g = 3$) is given by the equation

$$F(x, y, z) = x^3y + y^3z + z^3x. \tag{6}$$

In this case $\nu_1 = 3$, $\nu_2 = 5$, $\nu_3 = 24$.

Indeed, $[1, 0, 0]$, $[0, 1, 0]$ and $[0, 0, 1]$ are the only points of C that satisfy $xyz = 0$ (the first two are at infinity). If $xyz \neq 0$, then we can look at the affine curve $C_z = x^3y + y^3 + x$. Over $\mathbb{F}_2$ it is clear that there are no more points, hence $\nu_1 = 3$. Over $\mathbb{F}_4$, there are two more points: $(\alpha, \alpha^2, 1)$ and $(\alpha^2, \alpha, 1)$, where $\alpha^2 = \alpha + 1$, and so $\nu_2 = 5$. To get ν_3, let $\mathbb{F}_8$ be generated by β with $\beta^3 = \beta + 1$. Since $y^3 = y^{10}$, on dividing C_z by y^3 we get $(x/y^3)^3 + 1 + x/y^3 = 0$. Since $\xi^3 + \xi + 1 = 0$ has three solutions in $\mathbb{F}_8$ $(\beta, \beta^2, \beta^4)$, we conclude that C_z has $7 \times 3 = 21$ poins other than $(0, 0)$ that are $\mathbb{F}_8$-rational and therefore $\nu_3 = 24$. With this, the values for ν_r supplied by XN (for $r \leqslant 12$) are the following:

r	1	2	3	4	5	6	7	8	9	10	11	12
ν_r	3	5	24	17	33	38	129	257	528	1025	2049	4238

Over $\mathbb{F}_5$, one finds that $\nu_1 = 6$, $\nu_2 = 26$ and $\nu_3 = 126$. With this, we get a similar table (for $r = 1, \ldots, 9$):

r	1	2	3	4	5	6	7	8	9
ν_r	6	26	126	626	3126	16376	78126	390626	1953126

```
def Deuring_offsets(q):
    P = prime_factors(q) # prime_factors(12) => [2, 2, 3]
    p = P[0]; n = len(P)
    m = int(2*sqrt(q))
    D = [t for t in range(-m,m+1) if gcd(p,t)==1]
    if n%2==0:
        r = p**(n//2)
        D += [-2*r,2*r]
        if p%3 != 1:
            D += [-r,r]
    if n%2 and (p==2 or p==3):
        r = p**((n+1)//2)
        D += [-r,r]
    if n%2 or (n%2==0 and p%4!=1):
        D += [0]
    return sorted([t for t in D])
```

```
def Deuring_set(q):
    D =Deuring_offsets(q)
    return [t+q+1 for t in D]
```

Practice: Experience with the notebook wit_ratpoints.

References I

[1] H. Behnke, F. Bachmann, K. Fladt, and H. Kunle (eds).

Fundamentals of Mathematics, vol. 2.

The MIT Press, 1974.

Edited with the assistance of H. Gerike, F. Hohenbert, G. Pickert, H. Rau; translated to English from the second German edition *Grundzüge der Mathematik*, Vandenhoeck & Ruppert, 1967, 1971. Especially relevant chapters: 12, *Eralangen program and higher geometry* (H. Kunle and K. Fladt) and 13, *Group theory and geometry* (H. Freudenthal and H.-G. Steiner).

References II

[2] Jonathan Cameron and Joan Lasenby.

Oriented conformal geometric algebra.

Advances in applied Clifford algebras, 18(3-4):523–538, 2008.

[3] T. E Cecil.

Lie sphere geometry. With applications to submanifolds.

Springer, 2008.

[4] Richard Courant and Herbert Robbins.

Was ist mathematik? An elementary approach to ideas and methods (second edition).

Oxford University Press, 1996.

A revision by Ian Stewart of the 1941 edition.

References III

[5] H. S. M. Coxeter and S. L. Greitzer.

Geometry revisited, volume 19 of *New Mathematical Library*.

MAA, 1967.

[6] W. Fulton.

Intersection theory, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge*.

Springer-Verlag, 1984.

Second edition: Springer, 1998.

References IV

[7] R. Hartshorne.

Algebraic geometry, volume 52 of *Graduate Texts in Mathematics*.

Springer-Verlag, 1977.

Corrected eighth printing 1997.

[8] Udo Hertrich-Jeromin.

Introduction to Möbius differential geometry, volume 300 of *LMS Lecture Notes*.

Cambridge University Press, 2003.

[9] Vladimir V Kisil.

Lectures on Moebius-Lie Geometry and its Extension, 2018.

arXivpreprintarXiv:1811.10499.

References V

[10] S. L. Kleiman.

The enumerative theory of singularities.

In P. Holm, editor, *Real and Complex Singularities (Oslo 1976)*, pages 297–396. Sijthoff and Noordhoff, 1977.

Proceedings of the Nordic Summer School/NAVF Symposium in Mathematics, Oslo, August 5-25, 1976.

[11] Carlile Lavor, Sebastià Xambó-Descamps, and Isiah Zaplana.

A Geometric Algebra Invitation to Space-Time Physics, Robotics and Molecular Geometry.

SBMA/Springerbrief. Springer, 2018.

References VI

[12] S. Molina, N. Sayols, and S. Xambó-Descamps.

A bootstrap for the number of F_{q^r}-rational points on a curve over F_q, 2017.

https://arxiv.org/abs/1704.04661.

[13] David Mumford, Caroline Series, and David Wright.

Indra's pearls: The vision of Felix Klein.

Cambridge University Press, 2002.

[14] Arkadij L Onishchik and Rolf Sulanke.

Projective and Cayley-Klein Geometries.

Springer Monographs in Mathematics. Springer, 2006.

References VII

[15] D. Pedoe.

A course of geometry for colleges and universities.

Cambridge University Press, 1970.

In 1988 Dover published and unabridge, corrected republication with the title *Geometry. A comprehensive course*.

[16] Jürgen Richter-Gebert and Thorsten Orendt.

Geometriekalküle.

Springer-Verlag, 2009.

References VIII

[17] J. G Semple.

On complete quadrics (I).

Journal of the London Mathematical Society, 23(4):258–267, 1948.

Part II: see [18].

[18] J. G. Semple.

On complete quadrics (II).

Journal of the London Mathematical Society, 27(3):280–287, 1952.

Part I: see [17].

References IX

[19] J.-P. Serre.

Nombre de points des courbes algébriques sur F_q.

Séminaire de Théorie des Nombres de Bordeaux 1982/83, 22, 1983.

Included in [22], number **129**, 664-668.

[20] J.-P. Serre.

Sur le nombre de points rationels d'une courbe algébrique sur un corps fini.

Comptes Rendues de l'Académie de Sciences de Paris, 296:397–402, 1983.

Included in [22], number **128**, 658-663.

References X

[21] J.-P. Serre.

Résumé des cours de 1983-1984.

Annuaire du Collège de France, pages 79–83, 1984.

Included in [22], number **132**, 701-705.

[22] J.-P. Serre.

Oeuvres, III (1972-1984).

Springer-Verlag, 1985.

References XI

[23] F. Severi.

Sul principio della conservazione del numero.

Rendiconti del Circolo Matematico di Palermo (1884-1940), 33(1):313–327, 1912.

Included in *Memorie Scelte*, 117-136.

[24] R. Sulanke.

Differential Geometry of the Möbius Space, I, 2019.

http://www-irm.mathematik.hu-berlin.de/~sulanke/diffgeo/moebius/mdg.pdf.

References XII

[25] Fernando Torres.

Algebraic curves with many points over finite fields.

Advances in algebraic geometry codes, 5:221, 2008.

[26] Gerard van der Geer.

Counting curves over finite fields.

Finite fields and their applications, 32:207–232, 2015.

[27] B. L. Van der Waerden.

Einführung in die algebraische Geometrie, volume 51 of *Grundleheren der Mathematischen Wissenschaften*.

Springer-Verlag, 1939.

Second edition 1972.

References XIII

[28] B. L. Van der Waerden.

Moderne Algebra.

Springer, 1950.

[29] B. L. Van der Waerden.

The foundation of algebraic geometry from Severi to André Weil.

Archive for History of Exact Sciences, 7(3):171–180, 1971.

[30] R. J. Walker.

Algebraic curves.

Princeton University Press, 1950.

References XIV

[31] Wikipedia.

Problem of Apollonius, 2019-12-27.

https://en.wikipedia.org/wiki/Problem_of_Apollonius.

[32] S. Xambó-Descamps.

Francesco Severi and the principle of conservation of number.

Rendiconti del Circolo Matematico di Palermo, Serie II, 36:255–277, 1994.

This issue of the Rendiconti collects papers presented at the conference *Algebra e Geometria* (1860-1940): *Il contibuto italiano* held in Cortona, 4-8 May, 1992.

References XV

[33] S. Xambó-Descamps.

Using intersection theory.

Number 7 in Aportaciones Matemáticas, Nivel Avanzado. Sociedad Matemática Mexicana, 1996.

122 pp.

[34] S. Xambó-Descamps.

Conformal Geometric Algebra—An introduction, 2016.

Talk at the minicourse *Geometric Algebra Techniques in Mathematics, Physics and Engineering* held at IMUVA, 16-20 May, 2016.

References XVI

[35] S. Xambó-Descamps, J. M. Miret, and N. Sayols.

Intersection Theory and Enumerative Geometry—A Computational Primer.

Universitext. Springer, 2020.

Updated and extended edition of [33] enriched with a computational environment, of.

[36] B. J. Zlobec and N. M. Kosta.

Configurations of cycles and the Apollonius problem.

The Rocky Mountain Journal of Mathematics, pages 725–744, 2001.