On the Mechanization of Straightedge and Compass Constructions

Pascal Schreck

On the Mechanization of Straightedge and Compass Constructions

Pascal Schreck

E-mail: schreck@unistra.fr

Abstract The geometric constructions obtained with only straightedge and compass are famous and play a special role in the development of geometry. On the one hand, the constructibility of figures is a key ingredient in Euclid geometry and, on the other hand, unconstructibility gave birth to famous open problems of the ancient Greece which were unlocked only in the nineteenth century using discoveries in algebra. This paper discusses the mechanization of straightedge and compass constructions. It focuses on the algebraic approaches and presents two methods which are implemented; one is due to Lebesgue and the other one was jointly designed by Gao and Chou. Some links between the algebraic approach of constructions and synthetic geometry are described.

1 Introduction

Apart from their practical use in architectural or mechanical design, geometric constructions play a very special role in mathematics. Historically they are the constructive face of the axiomatization of geometry by the ancient Greeks. In addition to the fact that the result of a construction problem is an algorithm, one can see this fundamental aspect of Greek geometry as a middle ground with the constructive Chinese point of view of mathematics [Chemla and Guo(2005), Wu(2008)]. Despite its antiquity, this constructive design of geometry sounds singularly in the modern conception of mathematics and particularly in the context of computational mathematics.

UFR de Mathématique et Informatique - ICube
7, rue René Descartes
67084, Strasbourg
France

The ancient Greeks considered straightedge and compass as effective tools for representing idealized lines and circles, then straightedge[1] and compass constructions, RC-constructions in short, gained a special status in geometry that remains to this day. This is especially true in education where they are an inexhaustible source of problems for exercising the imagination and the rigor of students, or as a recreational pastime [Wernick(1982),Euclidea(2016–2018)]. It is also worth citing educational software of dynamic geometry, like the precursor Cabri Géomètre and the renowned GeoGebra [Laborde and Strasser(1990), Hohenwarter and Fuchs(2004)], that made geometry more empirical and more accessible to students.

Interestingly, RC-construction are also famous because they gave rise to problems impossible to solve which were open for about two millennia. These problems were solved thanks to a radical change of point of view about geometry rooted in "Cartesianization" of geometry and progress in algebra with Galois results on solvability of polynomial equations. As often, it was useful to get out of a theory to obtain an impossibility result about that theory. These works stressed the difference between constructibility and construction: solving a problem with straightedge and compass immediately answers the question of constructibility, but not knowing a construction does not mean that a problem is not RC-constructible. Conversely, knowing that a problem is RC-constructible does not necessary gives a (usable) construction. In a previous work with Pascal Mathis [Schreck and Mathis(2016)], we exploited algebraic results to automatically check a whole corpus, namely the Wernick's and Connelly's lists, about RC-constructibility of triangle problems [Connelly(2009)]. We noticed that it is easier to show that a problem is RC-unconstructible than the opposite. And when we showed that a problem was RC-constructible, we sometimes had no idea about the geometric constructions. This paper discusses this issue by studying two constructive methods due to Henri Lebesgue and to Xiao-Shan Gao and Shang-Ching Chou.

It has to be noted that the ancient Greeks knew how to solve RC-unconstructible problems like angle trisection or doubling the cube by using smart tools to draw loci more powerful than lines and circles. Conversely, the folklore of geometric constructions contains several results about less powerful tools like, for instance, using a rusted compass instead of a compass, or only a compass and no straightedge. The former example is a classical problem for students in geometry, and the second one is also classical but far from obvious. But, radically different tools can be considered. With the work of Margharita P. Beloch in 1936 [Hull(2011)], origami, or rather computational origami, has regained popularity both from the practical/artistic and the mathematical points of view [Alperin(2000),Ida et al.(2015)Ida, Ghourabi, and Takahashi,Justin(1987)]. We do not discuss further these domains and we restrain ourselves to straightedge and compass constructions.

The rest of the paper is organized as follows. Section 2 presents the domain of straightedge and compass constructions and its two synthetic and algebraic faces. Section 3 focuses on the algebraic aspects of constructions, in particular the use of the Wu method and the works of Lebesgue and Gao & Chou. Section 4 describes

---

[1] Some authors use the word ruler for straightedge giving the shortcut RC-construction used throughout this text.

some examples of application and briefly discusses the qualities and defects of the algebraic approach.

2 Geometric RC-constructions

Geometric RC-constructions are known for millennia. But, despite polished mathematical definitions, they must be carefully specified when it comes to mechanizing them. This section discusses the specific features and how to handle them in a computational approach.

2.1 Definition and discussion

First, RC-constructibility can be classically defined as follows (this definition comes from a French book dedicated to mathematics teachers [Carréga(1981)]):

Definition 1 (RC-constructibility) Given a finite set of points $\mathcal{B} = \{B_0, \ldots, B_m\}$ in the Euclidean plane, a point P is *RC-constructible from the set* $\mathcal{B}$ if there is a finite set of points $\{P_0, \ldots, P_n\}$ such that $P = P_n$, $P_0 \in \mathcal{B}$ and every point P_i ($1 \leq i \leq n$) is either a point of $\mathcal{B}$ or is at the intersection either of two lines, or of a line and a circle, or of two circles, themselves obtained as follows:

- any considered line passes through two distinct points from the set $\{P_0, \ldots, P_{i-1}\}$;
- any considered circle has its center in the set $\{P_0, \ldots, P_{i-1}\}$ and its radius is equal to the distance $P_j P_k$ for some $j < i$ and $k < i$.

The sequence of these points with their basic constructions in terms of intersections between lines and circles is called a RC-construction of point P.
A line is said RC-constructible from $\mathcal{B}$ if it contains two distinct points RC-constructible from $\mathcal{B}$.
A circle is said RC-constructible from $\mathcal{B}$ if its center is RC-constructible from $\mathcal{B}$ and there are two points M and N RC-constructible from $\mathcal{B}$ such that MN equals its radius.

Consequently, for proving that a point or a line or a circle is RC-constructible from $\mathcal{B}$, it suffices to define such a sequence of points, in addition the proof should exhibit the lines and circles used for defining these points, and also a proof of correctness. In many textbooks, the following example comes just after that definition:

> Given a line l and a point A, it is possible to construct with straightedge and compass the line m perpendicular to l and passing through A.

The construction is easy, but the problem does not fit this definition. In fact, we have to construct or to choose *two* distinct points on l, to use them for the construction and to *prove* that the result does not depend on that choice. Usually, basic axioms for geometry impose that a line has to contain at least two or three points, or in other words, within a constructive approach, we suppose that we have a function yielding two points from a line: classically these points do not have to be RC-constructible from $\mathcal{B}$ since they are forgotten after the construction, but when it comes to discussing what is the underlying geometry this issue

becomes questionable. We do not press this point further, but if one wants to implement a software for RC-construction, this question has to be answered. In most of the frameworks for RC-construction, this question is side-stepped by giving this construction as a primitive.

A construction problem therefore consists in a specification of a figure made of geometric relations between given points, lines or circles and sought points, lines or circles. Now, the question is "what kind of relations?". For instance, if we consider technical drawing, another domain where geometric constructions were widely used, these relations are currently called geometric constraints and are mainly related to dimensions: there are standards in this regard and CAD softwares take them into account. But the fun, in mathematics, is to impose original constraints: for instance, how to draw the bisectors of two lines which meets outside the sheet of paper? Or how to draw a perpendicular with a wood square having a broken corner? This kind of relations also tightly relies on the subtended geometry. For instance, Wu's metric geometry does not consider an order on the points of a line, then the notions of orientations are out of reach. On the other hand, Wernick's and Connelly's corpora deal with some remarkable points of the triangle and their relations with its vertexes in the $\mathbb{R}^2$ Euclidean plane. These considerations must be taken into account especially when it comes to using algebra in this context.

Also, the initial points can be given in an absolute way, say by giving their coordinates in some reference system, or, alternatively, they can be given as parameters, or free points in the dynamic geometry parlance. The latter case is more problematic since the problem can be solved for some particular configurations and not for others. For instance, it is possible to cut the right angle in three using only straightedge and compass, but apart from a null set, it is not possible to do it for any angle. We face here a well known problem in rigidity theory or in mechanical geometry theorem proving where an assertion can be either generally true (that is true except for degenerate cases) or generally false, or even, true on parts/false on parts [Botana and Recio(2016)]. This also should be taken into consideration especially when algebra is involved.

Let us now turn to the question of the form of the expected result. We said in Definition 1, that the proof of the constructibility could be constituted by a RC-construction, that is, a sequence of points with their basic construction in terms of intersection between lines and circles. But having now, free points to consider, it could happen that:

  - the configuration of the free points leads to a degenerate case,
  - in the case of multiple intersection, like circle-circle intersection, both points lead to a solution or on the contrary, only one point leads to a solution (how to chose it?),
  - there are two or more different constructions producing different figures, some or all of them, meeting the requirements according to the parameters values.

Consider the following statement:

Statement 21 Two parallel lines l_1 and l_2, and three points A on l_1, B on l_2 and C being given in addition to a fixed length k, produce a RC-construction for a line L passing through C and cutting line l_1 in M and line l_2 in N such that $AM + BN = k$ (See Fig. 1).
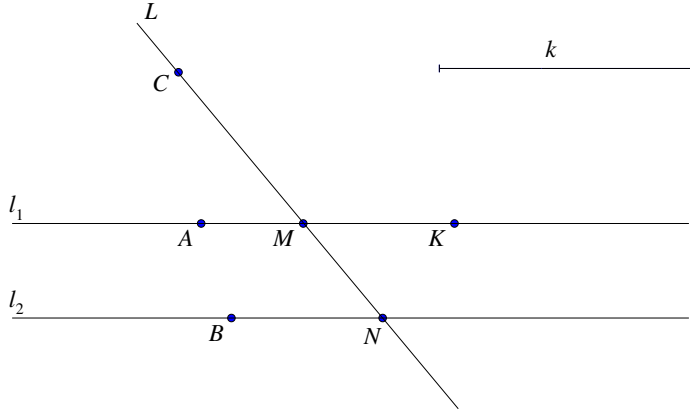
Fig. 1 Figure corresponding to Statement 21

This problem is *RC-solvable* if every solution can be constructed using only straightedge and compass from a base set containing lines l_1, l_2, points A, B and C, and two points giving length k.

The resolution is not complicated but a bit tricky. After adding a new point K on line l_1 such that $AK = k$, it is easy to see on the figure that $MKNB$ is a parallelogram, hence the midpoint I of segment BK should also be the midpoint of segment MN. The sought line is then line CI whose RC-construction is easy to get. In fact, this is a rough analysis of the problem, there are indeed several issues:

- what happens if $I = C$?
- more subtly, what happens if C is on the line parallel to l_1 through I?
- we choose one point K such that $AK = k$ but there is another point symmetrical *wrt A* meeting this requirement. Do we get the same solution with both choices?
- we said above that $MKNB$ is a parallelogram (without explanations), but it also could happen that $MKBN$ is a parallelogram (and $MKNB$ is a cross quadrangle). In this case, a solution is the line passing through point C and parallel to line BK.

The situation is a bit more complicated than expected. We have two kinds of constructions: one is using the midpoint of (M, N), let us call it construction of type I, and the other one is using the direction of line MN, construction of type d. Several cases can occur, we can have (See Fig. 2):

- no line L at all,
- two lines L_1 and L_2: one of type I and one of type d, or both of the same type I or d,
- infinitely many lines if $C = I$ or $C = I'$.

Back to RC-construction, we can see that, when line L specified by the statement exists, it is always RC-constructible. The problem is then RC-solvable and the very solution of Statement 21 is a procedure to construct all the possible lines L in every cases. This can be formalized by the notion of program of construction which is a formal way to express geometric constructions. With the previous example, we could get the program given on Table 1. This program is automatically
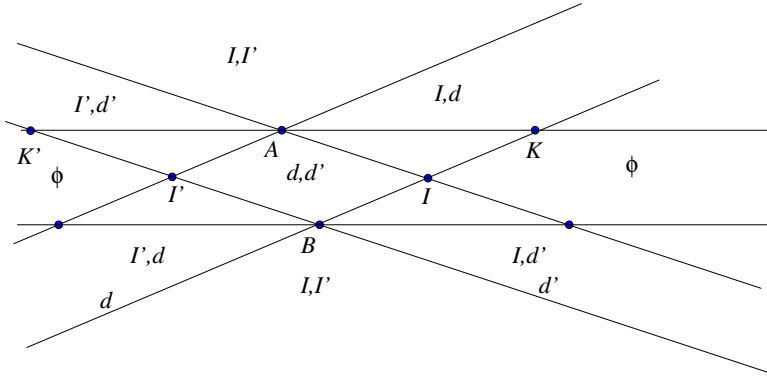
Fig. 2 Different areas where point C can be located according to the construction cases: I (resp. I', d, d') means that point I (resp. point I', direction d, direction d') is used in the RC-construction, $\emptyset$ indicates that there is no solution (constructible or not) in the area. If C equals I or I', there are infinitely many solutions. If C is on an oblique line there are two solutions on the frontier of two solution area and only one solution on a frontier with an area labeled by $\emptyset$.

produced by a Prolog software prototype called Progé that I implemented a long time ago during my PhD (see [Schreck(1993), Schreck(1994)] for more details).

The *ad-hoc* geometric programming language contains special control structures like conditional and kind of iterative instructions. It was designed to implement logical structures expressing solvability into procedures. We will see below, that it is possible to give it an algebraic meaning.

2.2 RC-(un)constructibility and algebra

Proving the impossibility of having such a program of construction is more problematic. Let us spend a moment about the notion of RC-unconstructibility (or RC-unsolvability for a problem). A problem is RC-unsolvable if there are non-degenerate real solutions which are not RC-constructible.

As said in the introduction, the domain of RC-constructions is famous because of unsolvable problems like squaring the circle or doubling the cube. These problems are related to the RC-construction of numbers. Let us recall the definition:

Definition 2 (RC-construction of numbers) Given a finite set of points $\mathcal{B} = \{B_0, \ldots, B_m\}$ in the Euclidean plane, a number a is said RC-constructible from $\mathcal{B}$ if one can construct using only straightedge and compass a point P whose abscissa is a. A number is RC-constructible (without mention of a base set) if it is RC-constructible from $\{O, I\}$, point O having coordinates $(0, 0)$, and I, $(1, 0)$.

It is not complicated to see that all the rational numbers are RC-constructible since there is a construction to perform the sum and the difference of any constructible numbers and then we are able to construct any integer from O and I (see Fig. 3, remark that the given construction adds algebraic distances and thus, it works for addition and substraction). On the same figure, we give a construction for the product of two constructible numbers –the construction of the quotient is
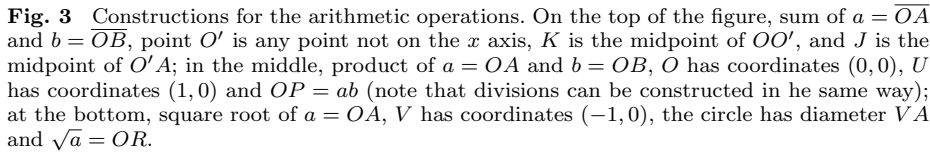
Construction Program

```
c := (given point)
di := (given direction)
a := (given point)
b := (given point)
k := (given length)
l1 := dpdir(a, di)
l2 := dpdir(b, di)
circle00 := ccr(a, k)
list00 := [intercl1(circle00, l1), intercl2(circle00, l1)]
for point00 in list00 do
  list01 := [pll(point00,m,b,n), pll(point00,m,n,b)]
  for case00 in list01 do
      if case00 = pll(point00, m, b, n) then
          len03 := dist(point00,b)
          if point00 dif b then
             point01 := mid(point00, b)
             line00 := sline(b, point00)
             len04 := dist(point01, c)
             if point01 diff c then
                l := sline(point01, c)
                m := interll(l, l1)
                n := interll(l, l2)
                end
             else fail
                end
             end
          else fail
             end
          end
       if case00 = pll(point00, m, n, b) then
           len05 := dist(b, point00)
           if b diff point00 then
              line05 := sline(b, point00)
              l := dpdir(c, dir06)
              m := interll(l, l1)
              n := interll(l, l2)
              end
           else
               fail
               end
           end
          else
            fail
            end
          end
  end
end
verify(m is_onl l1)
verify(n is_onl l2)
verify(m is_onl l)
verify(n is_onl l)
verify(c is_on l)
verify(dist(a,m) + dist(b, n) == k)
verify(l1 diff l2)
end
```

Table 1 A complete construction program automatically produced by software Progé. Notice that this is Prolog code, in fact a big Prolog term, and all the variables noted with uppercase in the statement are here in lower case. Also, the names of auxiliary objects (points, lines, . . .) are automatically given, for instance **point00** taken in **list00** corresponds to point K on the figure. Moreover, the existence of the intersection point of lines is not discussed in this program.

Fig. 3 Constructions for the arithmetic operations. On the top of the figure, sum of $a = \overline{OA}$ and $b = \overline{OB}$, point O' is any point not on the x axis, K is the midpoint of OO', and J is the midpoint of $O'A$; in the middle, product of $a = OA$ and $b = OB$, O has coordinates $(0,0)$, U has coordinates $(1,0)$ and $OP = ab$ (note that divisions can be constructed in he same way); at the bottom, square root of $a = OA$, V has coordinates $(-1,0)$, the circle has diameter VA and $\sqrt{a} = OR$.

very similar. A simple construction allows to graphically compute the square root of a constructible number. With these constructions we get that the set of RC-constructible numbers together with addition and multiplication is an Euclidean[2] subfield of $\mathbb{R}$. A more precise result expresses that this field is the smaller Euclidean subfield of $\mathbb{R}$.

There are two famous results about RC-constructible numbers. The first one is related to the previous observation:

Theorem 1 (Wantzel) *A number a is RC-constructible if and only if it can be expressed by an arithmetic expression with radicals, that is, involving only numbers in $\mathbb{Q}$, arithmetic operations and square root extractions.*

A consequence of this theorem is known as Wantzel's result which states that any number a RC-constructible is algebraic and $[\mathbb{Q}[a] : \mathbb{Q}] = 2^n$ for some n. This result is sufficient to prove that one cannot double the unit cube using only straight-edge and compass, that the trisection of $\frac{\pi}{3}$ angle is RC-unsolvable, and since π is not algebraic (proved by Lindenmann in 1882), that squaring the circle is also impossible.

---

[2] Euclidean means stable by the square root operation.

As noted before, we consider numbers constructible from $\{O, I\}$ and then, polynomials with coefficients in $\mathbb{Q}$ (or $\mathbb{Z}$ without loss of generality). This extensible to some field F which classically is a transcendental extension of $\mathbb{Q}$ of the form $\mathbb{Q}(u_1, \ldots, u_m)$ where $u_1, \ldots, u_m$ are parameters. Also note that Wantzel's result only gives a necessary condition and cannot be used to prove that a number is RC-constructible. The following theorem is a necessary and sufficient condition for a number to be RC-constructible (see [Stewart(2003)] for instance).

Theorem 2 (Galois) *An algebraic number on F is constructible if and only if the splitting field of its minimal polynomial P, is an extension of degree 2^m for some m over F. The degree of this extension, 2^m, is also the cardinal of the Galois group of P.*

The latter theorem is sufficient to prove both RC-constructibility and RC-unconstructibility of an algebraic number specified by its minimal polynomial and providing that we can compute the Galois group of this polynomial. In fact, this a key ingredient in the method used by the author and Mathis to automatically check and prove the RC-constructibility status of all the problems in both Wernick's and Connelly's corpora [Mathis and Schreck(2016)] which describe about 250 problems about triangle construction. But, when a problem is RC-solvable, Galois theorem does not give the result, that is, a procedure to construct the solutions using only straightedge and compass.

In the nineties, two methods were described and implemented to give an answer to this issue by describing a way to compute the algebraic expression –using only arithmetic and square root operations– of a constructible number. Having this expression, it is possible to translate it into elementary operations that can be performed using straightedge and compass.

The first one comes from lectures by Lebesgue in "Collège de France" in 1942 [Lebesgue(1950)] simplified and implemented by Chen in Maple. This work was the result of an end-of-studies internship on a subject directed by the author and Dufourd and, for now, only a master thesis is available [Chen(1992)]. The second one is due to Gao and Chou and it is more in the Chinese tradition reinvigorating by Wu [Wu(2008)]. It was published by Computer Aided Design journal (CAD, Elsevier) in 1998 [Gao and Chou(1998)].

It is to be noted that the problem of solving a RC-solvable univariate polynomial has been addressed by Landau and Miller [Landau and Miller(1985)] in the case where the coefficient field is $\mathbb{Q}$. But, their algorithm is focused on univariate polynomials in $\mathbb{Q}[X]$ and does not extend to problems with parameters. Moreover, as far as we know, it has no been implemented yet. To our knowledge, the methods of Lebesgue and Gao-Chou are the only methods which fully address the problem of RC-solvability.

The next sections present these works and compare them on some simple examples.

3 RC-construction and algebra

In the previous section, we focused on the algebraic characterization of RC-constructible numbers. Now, we want to practically solve more general construction problems by using algebra. It is worth to notice that we place ourselves within the geometrical framework described by Wu, namely the metric geometry: we only

consider statements that can be translated into polynomial equations. In a corpus approach like the problems from the lists of Wernick and Connelly, the translation can be automatically done [Schreck and Mathis(2016)].

Thus, a RC-construction problem becomes an algebraic system to be solved using only arithmetic and square root operations on a given field K which usually is a finite extension of $\mathbb{Q}$: in the following, we assume that $K = \mathbb{Q}(u_1, \ldots, u_m)$ where $u_1, \ldots, u_m$ are independent parameters. But treating an algebraic system is not the same as treating a single polynomial equation, and the first step consists in yielding equivalent triangular systems.

At this point, we need to ask ourselves if the needed operations are computationally feasible.

3.1 Computatbility

For commodity, we define the notion of RP-computability:

Definition 3 (RP-computability) A field F is said RP-computable if and only if:

- there are data structures for representing the elements of F,
- there are algorithms for computing the arithmetic operations on F,
- there are algorithms for solving in F every polynomial equation in $F[X]$.

This definition means that such a field F can effectively be implemented and, given a polynomial with coefficients in F, we can compute all its roots belonging to F.

It is obvious that every finite field is RP-computable. The first interesting RP-computable field is $\mathbb{Q}$: data structures and algorithms for arithmetic operations are obvious, and it is well known that the rational roots of polynomial $a_n x^n + \ldots a_0$ whose coefficients are in $\mathbb{Z}$, are of the form p/q where p is a divisor of a_0 and q a divisor of a_n. Using triangularization algorithms, is not difficult to prove the following theorem:

Theorem 3 *A field F is RP-computable if and only if there is a factorization algorithm in $F[X]$.*

We then have the classical result:

Theorem 4 *Let $K \subset F$ be a field extension and $\mu \in F$ be either transcendental or specified by its minimal polynomial. If K is RP-computable then $K(\mu)$ is also computable.*

Indeed, if μ is algebraic we can then use its minimal polynomial for the computations including the factorization of polynomials (this latter proof is very close to the Lebesgue's technique used below in section 3.3). And if μ is transcendental, the factorization process is the very same than in $\mathbb{Q}$.

Then, $K = \mathbb{Q}(u_1, \ldots, u_m)$ where $u_1, \ldots, u_m$ is RP-computable and the finite extensions of K are also RP-computable.

We can now go back to the RC-solvability problem.

3.2 Triangularization

In Lebesgue's book, the question of the triangularization is not well developed. But recall that there was no computer at that time and he only described a theoretical method as a proof of concept. For him, the progressive elimination of variables can be done by successive uses of Euclidean division by embedding $K[X_1, \ldots X_i]$ in $K(X_1, \ldots X_{i-1})[X_i]$, that is the Euclidean domain of polynomials with coefficients in the field $K(X_1, \ldots X_{i-1})$, thus avoiding to consider the initials of the polynomial which is not very accurate as we know it now. Moreover, after that phase, each polynomial had to be factorized since Galois theory considers irreducible polynomials.

A more disciplined approach uses the Wu-Ritt's method to produce irreducible ascending sets [Wu(1984),Chou(1988)]. More precisely, if S is the given system, the method produces k triangular systems $T_1, \ldots T_k$ such that

$$V(S) = V(T_1) \cup V(T_2) \ldots \cup V(T_k)$$

There are several papers on the subject and elimination theory, see for instance [Kalkbrener(1993),Kapur and Saxena(1995),Buchberger and Winkler(1998)] and a recent comparison in [Wang(2016)]. In the following, we will use the regular chains [Aubry et al.(1999)Aubry, Lazard, and Moreno-Maza] which have all the required properties, in particular by producing irreducible components, for Galois's theory. More particularly, we use the Maple RegularChains tools which are implemented by Lemaire, Moreno Maza and Xie [Lemaire et al.(2005)Lemaire, Maza, and Xie]. Then each triangular system has to be examined separately. For each non degenerate system with real solutions, T_i, we have to solve the equation by beginning with the equations with least unknowns and reporting the found values in the remaining equation. The problem is then reduced to check if the roots of a polynomial are RC-constructible and to compute them. Knowing the Galois group of a polynomial does not allow to straightforwardly compute its constructible roots. On the contrary, the two algorithms presented below take parameters into account and can be used to both check the RC-solvability and formally compute the solutions.

3.3 Lebesgue's method

Original Lebesgue's method consists in decomposing a polynomial with a high degree so called the "resolving polynomial"[3]. This polynomial is built from an irreducible polynomial to be solved. In 1992, Chen with Carayol from the University of Strasbourg showed that it is useless to consider that polynomial. In fact, they proved that:

Theorem 5 (Chen and Carayol) *Let x be an algebraic number on a field K such that $\mathbb{Q} \subset K$ and P be its minimal polynomial. x is RC-constructible if and only if there is a number r in K such that P is decomposable on $K(\sqrt{r})$.*

---

[3] Résolvante de Galois in French

Thus, having a minimal polynomial (that is an irreducible polynomial with leading coefficient equal to 1) P, one tries to decompose P into two factors. We present the method with a simple example.

Consider $P(x) = x^4 + 2x - 2$, which is irreducible, and $K = \mathbb{Q}$, we search $r \in \mathbb{Q}$ and $r > 0$ such that there is a divisor of P in $K(\sqrt{r})[X]$.

If P has a factor of degree 1, it means that it has a root of the form $a\sqrt{r} + b$. Thus, $-a\sqrt{r} + b$ is also a root and then $x^2 - 2bx + a^2r + b^2$ should be a factor in $\mathbb{Q}[X]$ of P. But P is irreducible. It is then useless to search factors of degree 1.

Then, we search a divisor of degree 2, that is, of the form $F(x) = x^2 + (a + d\sqrt{r})x + b\sqrt{r} + c$. Remark that, since we can chose either d or b equal to 1 or -1, we have to add the equation $(d^2 - 1)(b^2 - 1) = 0$. In the following, for the sake of simplicity, we chose $d = 1$ forgetting solutions with $d = 0$ and $d = -1$ if any (we will see below that the case where $d = -1$ can be avoided). When we divide P by F the remainder should vanish everywhere. We get the polynomial (remember that we put $d = 1$):

$$((-3a + 2b)r + (-3a^2 + 2ab + 2c - r)\sqrt{r} - a^3 + 2ac + 2)x$$
$$(-2ab + b^2 - c)r + (-a^2b - 2ac + 2bc - br)\sqrt{r} - a^2c + c^2 - 2$$

since we want this polynomial to be null, we have the four equations:

$$\begin{cases} -3a^2 + 2ab + 2c - r = 0 \\ -a^3 + 2ac - 3ar + 2br + 2 = 0 \\ -a^2b - 2ac + 2bc - br = 0 \\ (-2ab + b^2 - c)r - a^2c + c^2 - 2 = 0 \end{cases}$$

After elimination of a, c and r by triangularizing the system using regular chains, we have the following equations in two components:

$$b^4 - 2b - 2 = 0$$

or, in the second component

$$4b^3 + 8b^2 + 1 = 0$$

where factor $4b^3 + 8b^2 + 1$ is remarkable (see below). It is also interesting to note that a factor very similar to the initial equation appears: $b^4 - 2b - 2$, but this time we are not seeking for RC-solvability, we only want to know if it admits rational solutions. It is easy to see that none of the equations has rational roots. Checking the other cases: $b = \pm 1$ and $d = -1$ leads to the same systems. The equation is then not RC-solvable.

Let us try a RC-solvable case and consider the polynomial $x^4 + 2x^3 - 3x^2 - 2x + 1$. After dividing it by $x^2 + (a + \sqrt{r})x + b\sqrt{r} + c$ we get the system:

$$\begin{cases} -a^2b + 2ab - 2ac + 2bc - br + 3b + 2c = 0 \\ (-2ab + b^2 + 2b - c)r - a^2c + 2ac + c^2 + 3c + 1 = 0 \\ -3a^2 + 2ab + 4a - 2b + 2c - r + 3 = 0 \\ (-3a + 2b + 2)r - a^3 + 2a^2 + 2ac + 3a - 2c - 2 = 0 \end{cases}$$

Then using regular chains, we find three irreducible components: two of them have no rational roots and the third one admits the single solution $a = 1, b = 0, c =$

$-1, r = 2$ giving the factor $x^2 + (1 + \sqrt{2})x - 1$. The other factor is $x^2 + (1 - \sqrt{2})x - 1$. The four solutions of these equations are of the form:

$$-(1/2)\sqrt{2} - 1/2 \pm (1/2)\sqrt{7 \pm 2\sqrt{2}} \ .$$

This method immediately extends to higher degree by searching factors of degree 2, 3, ... with an Euclidean division and making the remainder vanish: a factor F of degree k of $P(x)$ in $K[\sqrt{r}]$ is of the form:

$$x^k + m_{k-1}x^{k-1} + \ldots m_0 + \sqrt{r}(n_{k-1}x^{k-1} + \ldots n_0) \ .$$

And the remainder of P by the division by F is a polynomial of the form:

$$(A_{k-1}(m,n)\sqrt{r} + B_{k-1}(m,n))x^{k-1} + \ldots A_0(m,n)\sqrt{r} + B_0(m,n)$$

where $m = (m_0, \ldots m_{k-1})$, $n = (n_0, \ldots n_{k-1})$ and, $A_i(m,n)$ and $B_i(m,n)$ are polynomials with coefficient in K. This remainder equals the null polynomial if and only if F is a factor of P. This leads to an algebraic system with $2k + 1$ and $2k$ equations: we just add the equation $(n_0 - 1)(n_1 - 1) \ldots (n_{k-1} - 1) = 0$ as we did in our example. Now, we have to solve this system *in* K which, by chance, is RP-computable.

If we find some solution in r which permits the factorization, we continue with each factors until the polynomial is discomposed in factors of degree 1 [Lebesgue(1950), Chen(1992)].

3.4 Gao and Chou's method

Gao and Chou used another characterization of RC-constructible numbers:

Theorem 6 *Let K be a field as in the previous theorem and p be an algebraic number on K. p is RC-constructible if and only if there is a sequence of numbers $\alpha_1, \ldots \alpha_n$ such that*

- $[K(\alpha_1) : K] = 2$,
- $[K(\alpha_{i+1}, \ldots, \alpha_1) : K(\alpha_i, \ldots, \alpha_1)] = 2$, *for $i = 1, \ldots n - 1$,*
- $p = \alpha_n$

In our case, saying that a root p of polynomial $P(x) = x^4 + 2x - 2$ means that the algebraic system has $x_2 = p$ as solution (and $x_1 = \alpha_1$ with the notations of the above theorem):

$$\begin{cases} x_1^2 - r = 0 \\ x_2^2 + (x_1 + a)x_2 + bx_1 + c = 0 \end{cases}$$

where r, a, b, c are in $\mathbb{Q}$ and all the variables are unknowns. But, eliminating x_1 in this system leads to the minimal polynomial of p which is $P(x)$. It then comes:

$$x^4 + 2x - 2 \equiv x^4 + 2ax^3 + (-r + 2c + a^2)x^2 + (2ac - 2br)x - b^2r + c^2 \ .$$

Symbol $\equiv$ stands for equality of polynomials. Thus coefficients of both polynomials can be identified, and we get:

$$\begin{cases} 2a = 0 \\ -r + 2c + a^2 = 0 \\ -2br + 2ac - 2 = 0 \\ -b^2r + c^2 + 2 = 0 \end{cases}$$

Eliminating a, r and c leads to the equation $b^4(4b^3 + 8b^2 + 1) = 0$ (*). The obvious solution $b = 0$ gives by replacement the equation $c^2 + 2 = 0$ which has no rational solution. The second factor $4b^3 + 8b^2 + 1$ has not rational root. Thus the polynomial P is not solvable by square radicals.

For the RC-solvable polynomial $x^4 + 2x^3 - 3x^2 - 2x + 1$, the identification with the polynomial $x^4 + 2ax^3 + (a^2 + 2c - r)x^2 + (2(ac - br))x - rb^2 + c^2$ gives the system:

$$\begin{cases} b^2r - c^2 + 1 = 0 \\ 2 - 2a = 0 \\ -a^2 - 2c + r - 3 = 0 \\ -2ac + 2br - 2 = 0 \end{cases}$$

The triangularization yields two irreducible systems: the first one does not have any rational solution and the second one correspond to the solution found by Lebesgue's method.

This method is extended to higher degrees but even for polynomial of degree 8, the system to be solved is very complicated.

3.5 Comparison of the two methods with an example

Both methods are quite similar but Gao-Chou method seems more efficient than the Lebesgue's one, at least for the quartic equations. But the idea of factorizing the polynomial was not fully exploited by Lebesgue and computing the remainder brings complications.

Let us re-examine the first example where $P(x) = x^4 + 2x - 2$.

Using conjugation, we can see that if this polynomial is reducible in $\mathbb{Q}(\sqrt{r})[x]$, we have:

$$x^4 + 2x - 2 \equiv (x^2 + (a + \sqrt{r})x + b\sqrt{r} + c)(x^2 + (a - \sqrt{r})x - b\sqrt{r} + c)$$

identifying the coefficients, we get the system:

$$\begin{cases} 2a = 0 \\ a^2 + 2c - r = 0 \\ 2ac - 2br - 2 = 0 \\ -b^2r + c^2 + 2 = 0 \end{cases}$$

which is exactly the same system as in Gao-Chou method. The comparison for higher degrees is difficult because the polynomials found are very complicated. We guess that this idea of factorizing the minimal polynomial by identification could lead to some simplifications, but this is a subject for future research.

4 Examples and further discussions

In the previous sections, we only give tiny examples, without parameters, and we observe that the results are complicated. We will see these methods at work on some classical examples of construction problems.

4.1 A simple example

Let us begin with Example 21 of section 2. In order to translate the problem into algebra, we have to choose the coordinate system. We fix point B to coordinates $(0,0)$ and line l_2 will be the x-axis. Then, as point A can be chosen almost anywhere, it has coordinates (p_2, p_3) where p_i are parameters. It is the same for C whose coordinates are (p_4, p_5). The last parameters correspond to the sum of distances $AM + BN$ which is fixed to be equal to p_1 (that is $k = p_1$, we change the name for the sake of homogeneity). Then, points M and N are respectively located at (x_1, p_3) and $(x_2, 0)$.

Expressing that points C, M and N are collinear is straightforward and corresponds to the polynomial:

$$f_1 : (x_2 - x_1)p_5 - p_3(x_2 - p_4) \ .$$

It is also not difficult to translate the constraint $AM + BN = p_1$, and we get:

$$f_2 : (x_1 - p_2)^4 + x_2^4 + p_1^4 - 2((x_1 - p_2)^2 p_1^2 + x_2^2 p_1^2 + (x_1 - p_2)^2 x_2^2) \ .$$

After triangularization by using Maple's RegularChains tools, we obtain four irreducible systems. We describe and comment on the first and the third ones:

First system.

$$\begin{cases} (p_3 - p_5)x_2 - p_3 p_4 + x_1 p_5 = 0 \\ (p_3 - 2p_5)x_1 + (p_3 - p_5)p_1 + (-p_3 + p_5)p_2 + p_3 p_4 = 0 \end{cases}$$

with the additional conditions

$$\begin{cases} p_3 - 2p_5 \neq 0 \\ p_3 - p_5 \neq 0 \end{cases}$$

These conditions express that point C cannot be on l_1 and cannot be the line parallel to l_1 through I. This is a linear system and the solutions are easy to obtain:

$$x_1 = -\frac{p_1 p_3 - p_1 p_5 - p_2 p_3 + p_2 p_5 + p_3 p_4}{p_3 - 2p_5} \quad \text{and} \quad x_2 = \frac{p_1 p_5 - p_2 p_5 + p_3 p_4}{p_3 - 2p_5}$$

and we have $x_1 + x_2 = -p_1 + p_2$. This corresponds to a construction of type I with point K to the left of A. The second system (not described here) corresponds to the construction of type I with point K to the right of A. These constructions are valid even in the degenerate case where $l_1 = l_2$.

Third system

$$\begin{cases} (p_3 - p_5)x_2 + x_1 p_5 - p_3 p_4 = 0 \\ p_3 x_1 + (-p_3 + p_5)p_1 + (-p_3 + p_5)p_2 - p_3 p_4 = 0 \end{cases}$$

with the additional conditions

$$\begin{cases} p_3 \neq 0 \\ p_3 - p_5 \neq 0 \end{cases}$$

The conditions now express that point C cannot be on l_1 and line l_1 has to be distinct from line l_2. The solutions of that system are expressed by:

$$x_1 = \frac{p_1 p_3 - p_1 p_5 + p_2 p_3 - p_2 p_5 + p_3 p_4}{p_3} \quad \text{and} \quad x_2 = -\frac{p_1 p_5 + p_2 p_5 - p_3 p_4}{p_3}.$$

We observe here that $x_1 - x_2 = p_1 + p_2$ meaning that this corresponds to a construction of type d with point K to the right of A. The fourth system corresponds to a construction of type d with point K to the left of A.

We retrieve our four kinds of constructions, but the conditions are not as precise as the regions we found in Section 2. This is because using algebra we implicitly consider complex numbers and the distance between two points can be negative leading to more solutions than considering only real number.

This example illustrates the link between structuring the solution into different cases for both geometric construction programs and the decomposition of irreducible ideals but it does not show how the methods of section 3 can be used. This is the aim of the next example.

4.2 Example 119 from Wernick's list

This problem comes from a list of problems established by Wernick. The goal is to construct, if it is possible, a triangle being given three characteristic points among the vertices, the circumcenter, the midpoints of the sides and the gravity center, the feet of the altitudes and the orthocenter, and finally, the feet of the inner bisectors and the incenter. If a problem is not RC-solvable, a proof of its RC-unsolvability has to be produced. Problem 119 can be expressed as it follows:

Statement 41 (Wernick 119) Let I, G, H_a be three given points, construct points A, B and C such that I is the innercenter of triangle ABC, G its isobarycenter and H_a the foot of the altitude from A.

This problem is RC-solvable [Schreck and Mathis(2016)]. Our proof of its RC-solvability uses the algebraic approach. We first choose a cordinate system by taking the following coordinates: $I(0,0)$, $H_a(1,0)$ and $G(a,b)$ where a and b are parameters. Then, translating the constraints into algebraic expressions where $(x_A, y_A), (x_B, y_B)$ and (x_C, y_C) are the coordinates of points A, B and C to be constructed, we get the system:

$$\begin{cases} -x_A x_B^2 y_B - x_A x_B^2 y_C + 2 x_A x_B x_C y_B - x_A y_B^3 + x_A y_B^2 y_C + x_B^3 y_A + x_B^3 y_C \\ -x_B^2 x_C y_A - x_B^2 x_C y_B + x_B y_A y_B^2 - 2 x_B y_A y_B y_C + x_B y_B^2 y_C + x_C y_A y_B^2 - x_C y_B^3 = 0 \\ x_A^3 y_B + x_A^3 y_C - x_A^2 x_B y_A - x_A^2 x_B y_C - x_A^2 x_C y_A - x_A^2 x_C y_B + 2 x_A x_B x_C y_A \\ + x_A y_A^2 y_B + x_A y_A^2 y_C - 2 x_A y_A y_B y_C - x_B y_A^3 + x_B y_A^2 y_C - x_C y_A^3 + x_C y_A^2 y_B = 0 \\ (x_A - 1)(x_C - 1) + y_A y_C = 0 \\ (1 - x_B)(y_C - y_B) - y_B(x_B - x_C) = 0 \\ 3a - x_A - x_B - x_C = 0 \\ 3b - y_A - y_B - y_C = 0 \end{cases}$$

The triangularization of this system gives six irreducible systems with the last five being degenerate and the first one containing 5 linear equations and one polynomial equation with the single unknown y_C:

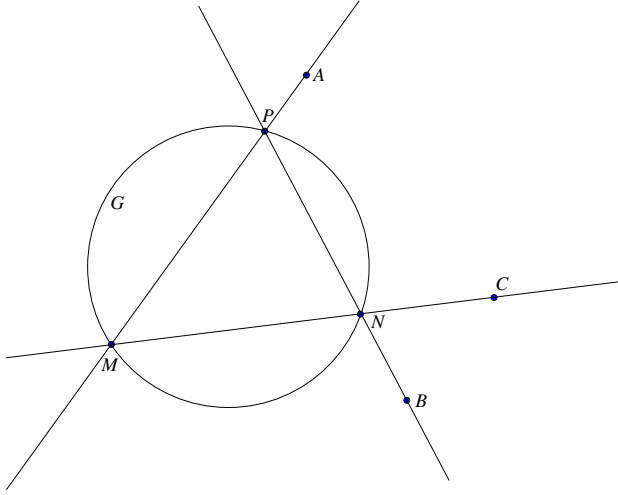$$P_{y_C} : c_4 y_C^4 + c_3 y_C^3 + c_2 y_C^2 + c_1 y_C + c_0 = 0$$

Fig. 4 The problem of Cramer and Castillon (Statement 42)

where
$c_4 = 19683a^9 - 59049a^8 + (78732b^2 + 61236)a^7 + (-183708b^2 - 20412)a^6 + (118098b^4 + 166212b^2 - 4374)a^5 + (-196830b^4 - 72900b^2 + 2754)a^4 + (78732b^6 + 148716b^4 + 10692b^2 + 324)a^3 + (-78732b^6 - 61236b^4 + 3564b^2 - 108)a^2 + (19683b^8 + 43740b^6 + 18954b^4 - 756b^2 - 21)a - 6561b^8 - 8748b^6 - 3078b^4 - 108b^2 - 1,$
the other coefficients $c_3, \ldots c_0$ being of the same kind. Maple is able to check if polynomial P_{y_C} is irreducible on $\mathbb{Q}(a,b)[X]$ and to compute its Galois group by identification [Hulpke(1999)]. The order of this group is 8, hence the problem is RC-constructible.

It is also possible to use Gao-Chou's method: considering quadratic polynomial P_{yc} the equation (*) of degree 3 described in section 3.4 is now a sum of 237 monomials in y, a and b where y is the unknown. This polynomial is reducible meaning that it has solutions in $\mathbb{Q}(a,b)$; hence the equation in y_C is RC-solvable and triangle ABC is RC-constructible. Maple gives a factor of this equation and then, a solution for y. This solution can be used to find r, as described above, and the coefficient of a quadratic equation with coefficients in $\mathbb{Q}(a,b,\sqrt{r})$ whose y_C is a solution. It is is clear that the exact formulation of this solution does not matter when it comes to producing a RC-construction.

The next example shows that this can be worst.

4.3 Cramer Castillon

The problem of Cramer-Castillon is a classical problem which is RC-constructible, and, even if the known construction is complicated, it is very simple to express:

Statement 42 (Cramer-Castillon) Let A, B and C be three given points and G be a given circle, construct three points M, N and P on G, such that, A is on line MP, B is on line NP and C is on line MN (See Fig. 4)

Without loss of generality, we can suppose that the radius of G equals 1 and its center has coordinates $(0,0)$. We can also suppose that C is on the x axis. Naming the coordinates of points, we get: $A(p_1, p_2), B(p_3, p_4), C(p_5, 0)$ and $M(x_1, x_2), N(x_3, x_4), P(x_5, x_6)$. Thus we have the system:

$$\begin{cases} f_1 : (x_1 - p_1)(x_6 - p_2) - (x_2 - p_2)(x_5 - p_1) \\ f_2 : (x_1 - p_5)x_4 - (x_3 - p_5)x_2 \\ f_3 : (x_5 - p_3)(x_4 - p_4) - (x_3 - p_3)(x_6 - p_4) \\ f_4 : x_1^2 + x_2^2 - 1 = 0 \\ f_5 : x_3^2 + x_4^2 - 1 = 0 \\ f_6 : x_5^2 + x_6^2 - 1 = 0 \end{cases}$$

But unfortunately, the triangularization of this system fails due to a lack of memory using a standard 2018 PC with 8Go of memory.

On the other hand, replacing the parameters by integers chosen at random, the triangularization is easily done and produce several degenerate cases (seven with my examples) and one containing only linear and quadratic equations. Thus, we can suspect that this problem is RC-constructible but we have no proof of it.

4.4 Discussion and last example

These examples highlight some aspects of the algebraic approach in RC-construction:

- algebra allows a systematic way to check if a problem is RC-solvable or not;
- when a problem is RC-constructible, it is possible to have the exact solutions and to extract a RC-construction;
- these techniques are in practice limited by a heavy complexity both in time and in space, and the current computer tools are unable to perform even the triangularization of a small algebraic system with parameters;

The picture is rather disturbing: the algebraic tools are very powerful but poorly usable to find the solutions. Let us say that, first it is important to know the existence of these methods as they fix some theoretical limits. Second, they are useful when it comes to proving RC-unconstructibility since they are actually almost the unique tool we have. For instance, with Pascal Mathis, we use them to automatically check the RC-constructibility (that is, proving RC-constructibility or finding counter-example) of both Wernick's and Connelly's lists. We then found the status, constructible, unconstructible or miss-constrained, for all the problems of these lists and resolving this way some open problems: most of these previously open problems are RC-unconstructible with some notable exceptions like Problem 119 of the Wernick's list and Problem 108 of that list which I present below. Notice that we proved that Problem 119 is RC-constructible and we are, in theory, able to produce a RC-construction, but the expression will be awful and not in the spirit of geometric construction.

Let us now present problem 108 of Wernick's list:

Statement 43 (Wernick 108) Let T_a, M_a and H be three given points, construct a triangle ABC such that H is its orthocenter, M_a the midpoint of edge BC and T_a the foot of the inner bisector from A
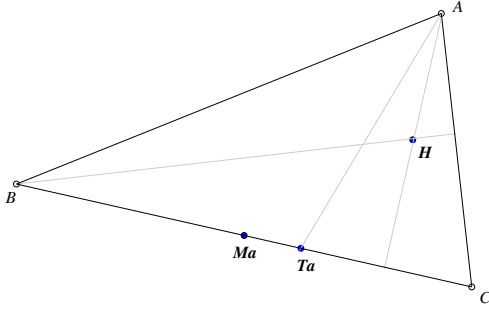
Fig. 5 Illustration of Statement 43: points Ma, Ta and H are given, and the problem is to construct the triangle ABC (the gray lines are the inner bisector from A and two altitudes, and they are figured here to recall the definitions of Ta and H).

Problem 108 is stated as RC-unconstructible in [Meyers(1996)]. But, using the algebraic tools described above, we find that this problem is RC-solvable. Moreover it is easy to prove this.

Thus, we consider the general case with the parameterized polynomial system by putting coordinates $(0,0)$ for point T_a, $(1,0)$ for point M_a and (a,b) for point H. The triangularization yields after filtering the following triangular system:

$$\begin{cases} x_C + x_B - 2 = 0 \\ -a^2 - by_A + x_B^2 + 2a - 2x_B = 0 \\ y_C = 0 \\ y_B = 0 \\ x_A - a = 0 \\ a^3 + aby_A - a^2 + y_A^2 = 0 \end{cases}$$

which is obviously RC-solvable, no need for Galois theory. The solutions are:

$$y_A = \frac{a}{2}\left(-b \pm \sqrt{b^2 - 4a + 4}\right)$$
$$x_C = 1 \pm \sqrt{a^2 + b.y_A - 2.a + 1}$$
$$x_B = 2 - x_C.$$

Hence, we can produce a construction with only straightedge and compass mimicking the calculi. For instance, the expression for y_A immediately translates into a geometric construction (See Fig. 6)

It can be observed that a simple calculation gives rise to a very complicated construction which has to be carefully handled. However, this construction is not satisfactory for the RC-construction fans since the fun of an elegant geometry reasoning is missing.

Now, in this example, we see that the quantity $b^2 - 4a + 4 = (2-a)^2 + b^2 - a^2$ plays a special role. This seems to indicate that the point P at location $(2-a, -b)$ could be interesting. Actually point P is a characteristic point of triangle ABC [4]: P is the symmetric of H with respect to M_a. This leads us to explore the figure very carefully and we find two useful properties:

---

[4] It is to be noted that there are thousands of such characteristic points as it can be seen in Clark Kimberling's Encyclopedia of Triangle Centers (`http://faculty.evansville.edu/ck6/encyclopedia/ETC.html`) [Narboux and Braun(2016)]

Fig. 6 Construction of $y_A = \frac{a}{2}(-b + \sqrt{b^2 - 4a + 4})$ by constructing the sequence of numbers b^2, $4a$, $b^2 - 4a$, $b^2 - 4a + 4$, $\sqrt{b^2 - 4a + 4}$, and so on.

– the inner angle bisector from A is also the inner angle bisector of the altitude AH and the ray AO where O is the circumcenter of triangle ABC.
– point P is also the symmetric of A with respect to O.

The construction is then as follows (see also Fig. 7). Line BC is known since point M_a and T_a are given. By projecting H on BC we have the foot H_a of the altitude from A and the altitude HH_a itself. From the first property above, T_a is the center of the circle Γ tangent to HH_a and AO, and passing through H_a. This circle is then constructible. Point P is also constructible: it is the symmetric of H wrt M_a. Since P is on line OA, this line passes through P and is tangent to circle Γ: line OP is constructible by using the circle with diameter PT_a. O is constructible as it is the intersection of this tangent and the perpendicular to line BC passing by M_a. We then have point A, the circumcircle of ABC and, finally, points B and C.

This suggests a heuristic approach to help solving a construction problem:

– check if the problem is RC-constructible or not,
– if it is, try to solve it algebraically and check the quantities under the square roots,
– ask for a characteristic point related to this quantities with data mining techniques (for instance, see [Song et al.(2017)Song, Wang, and Chen] for techniques of exploration of a figure and features extraction) and find the associated geometric relations.

Of course, the pertinence and the properties of the points found with heuristics have to be formally verified, for instance by using a CAS.
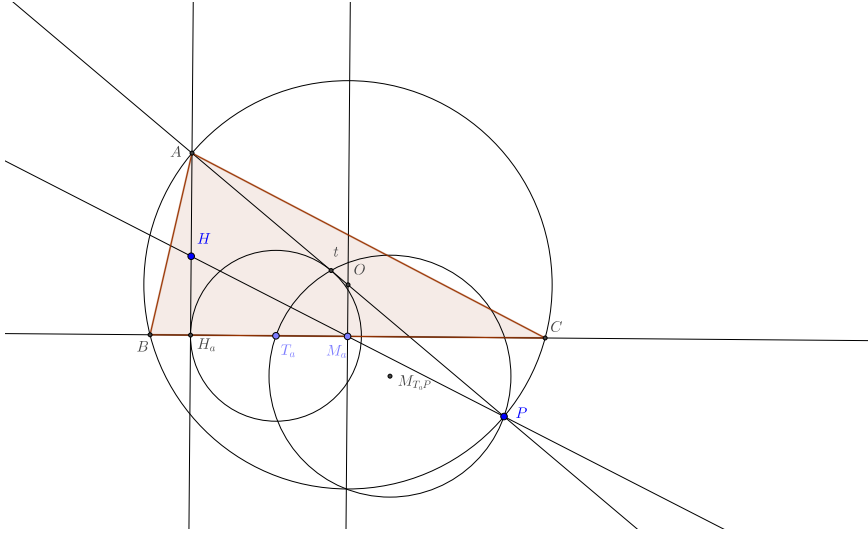
Fig. 7 A simple geometric construction for example 3, done by using point P.

5 Related works

On the one hand, considering the mathematical aspects of RC-constructions, thousands of articles and hundreds of books have been published over the centuries. In particular, following Lindenmann's result on the transcendence of π, the French "Académie des sciences" refused to publish the many false proofs of the problem of squaring the circle. Yet, they still receive papers claiming it solved! Recently, in the field of logic, especially intuitionistic logic in foundations of geometry, some works were already done within the framework of constructive geometry [Beeson(2012)].

On the other hand, as far as I know, very little has been done on the automation of ruler and compass constructions. Apart from the algebraic approaches described in this paper, the other works mainly follow a synthetic geometric approach.

The work of Scandura *et al.* seems to be the first one to describe a systematic way, with higher order geometric rules, to solve RC-constructions problems [Scandura et al.(1974)Scandura, Durnin, and Wulfeck II]. The geometric aspects are derived from Polya's work [Polya(1965)], but this work is more focused on pedagogical considerations about structural learning. To our knowledge, there is no implementation of this study.

In 1975, Buthion also worked on geometric construction and implemented his work in FORTRAN. Unfortunately, this work is only published in French [Buthion(1979)]. Without mentioning straightedge and compass, Aldefeld implement a synthetic geometric solver adapted to Computer Assisted Design, CAD, [Aldefeld(1988)] using ideas similar to those of Buthion. Also adopting a synthetic point of view, I developed in 1992 the notion of geometric universe and geometric construction program. This work is supported by a knowledge based system to exploit this notion to produce a highly parameterizable software able, *inter*

alia to solve RC-problems taking degenerate cases and multiple possibilities into account. This approach for solving construction problem was called universal approach [Schreck(1994)]. This work also was specialized by Mathis and Schreck to CAD in particular by using decomposition of problems invariant by direct isometries or even by similarities [Dufourd et al.(1998)Dufourd, Mathis, and Schreck, Schreck and Mathis(2006)].

It also worth citing the work of Gao *et al.* about the so-called reparameterization of 3D CAD-systems by using the so-called Locus Intersection Method (LIM) [Gao et al.(2002)Gao, Hoffmann, and Yang]. In this work, LIM is implemented by a simple solver whose result is in turn used by another solver based on a sampling method to numerically yield the solutions.

More recently Marinković and Janičić worked on a corpus approach in automatic RC-construction [Marinković and Janičić(2012)]. The problem is to fully automatically solve Wernick's corpus by giving a RC-construction when it is possible, and then to automatically prove that the construction really meets the statement specifications. For RC-unconstructible problems, they follow a reduction method to RC-irreducible problems [Schreck et al.(2016)Schreck, Marinkovic, and Janicic] or algebraic methods [Marinkovic et al.(2014)Marinkovic, Janicic, and Schreck].

Finally, Gulwani and his teams at Microsoft in program synthesis presented a very original approach using techniques of automatic program synthesis from a specification [Gulwani et al.(2011)Gulwani, Korthikanti, and Tiwari].

6 Conclusion

This paper mainly compares two different algebraic methods which theoretically are able to solve RC-construction problems, more precisely, able to detect if a problem is RC-solvable or not, and if it is, to express the solutions using only arithmetic operations and square root. We see on some examples that the algebraic tools used are effective in proving unconstructibility but when it comes to computing the solutions of constructible problems, they lack efficiency. However, some progress in information retrieval could possibly exploit the algebraic forms of the solutions, in simple cases, to retrieve relevant geometric constructions which is very helpful in the domain of computer aided education.

References

[Aldefeld(1988)] Aldefeld B (1988) Variations of geometries based on a geometric-reasoning method. Computer-Aided Design 20(3):117–126

[Alperin(2000)] Alperin RC (2000) A mathematical theory of origami constructions and numbers. New York Journal of Mathematics 6(119):133–148

[Aubry et al.(1999)Aubry, Lazard, and Moreno-Maza] Aubry P, Lazard D, Moreno-Maza M (1999) On the theories of triangular sets. J Symbolic Computation 28(2):105–124

[Beeson(2012)] Beeson M (2012) Logic of ruler and compass constructions. In: Cooper SB, Dawar A, Löwe B (eds) CiE, Springer, Lecture Notes in Computer Science, vol 7318, pp 46–55

[Botana and Recio(2016)] Botana F, Recio T (2016) On the unavoidable uncertainty of truth in dynamic geometry proving. Mathematics in Computer Science 10(1):5–25, DOI 10. 1007/s11786-016-0246-4, URL https://doi.org/10.1007/s11786-016-0246-4

[Buchberger and Winkler(1998)] Buchberger B, Winkler F (eds) (1998) Gröbner Bases and Applications. Cambridge University Press

[Buthion(1979)] Buthion M (1979) Un programme qui résout formellement des problèmes de constructions géométriques. RAIRO Informatique 13(1):73–106

[Carréga(1981)] Carréga JC (1981) Théorie des corps - La règle et le compas. Hermann Paris

[Chemla and Guo(2005)] Chemla K, Guo S (2005) Les neuf chapitres - Le classique mathmatique de la Chine ancienne et ses commentaires. Dunod

[Chen(1992)] Chen G (1992) Les constructions à la règle et au compas par une méthode algébrique. Tech. Rep. Master thesis, Université Louis Pasteur

[Chou(1988)] Chou SC (1988) An introduction to Wu's method for mechanical theorem proving in geometry. Journal of Automated Reasoning 4:237–267

[Connelly(2009)] Connelly H (2009) An extension of triangle constructions from located points. Forum Geometricorum 9:109–112

[Dufourd et al.(1998)Dufourd, Mathis, and Schreck] Dufourd J, Mathis P, Schreck P (1998) Geometric construction by assembling solved subfigures. Artif Intell 99(1):73–119, DOI 10. 1016/S0004-3702(97)00070-2, URL https://doi.org/10.1016/S0004-3702(97)00070-2

[Euclidea(2016–2018)] Euclidea (2016–2018) Euclidea: Euclidean constructions made fun to olay with. https://www.euclidea.xyz/

[Gao et al.(2002)Gao, Hoffmann, and Yang] Gao X, Hoffmann CM, Yang W (2002) Solving spatial basic geometric constraint configurations with locus intersection. In: Seidel H, Shapiro V, Lee K, Patrikalakis N (eds) Seventh ACM Symposium on Solid Modeling and Applications, Max-Planck-Institut für Informatik, Saarbrücken, Germany, June 17-21, 2002, ACM, pp 95–104, DOI 10.1145/566282.566299, URL http://doi.acm.org/10.1145/566282.566299

[Gao and Chou(1998)] Gao XS, Chou SC (1998) Solving geometric constraint systems. II. A symbolic approach and decision of Rc-constructibility. Computer Aided Design 30(2):115–122

[Gulwani et al.(2011)Gulwani, Korthikanti, and Tiwari] Gulwani S, Korthikanti VA, Tiwari A (2011) Synthesizing geometry constructions. In: Proceedings of the 32Nd ACM SIGPLAN Conference on Programming Language Design and Implementation, ACM, PLDI '11, pp 50–61

[Hohenwarter and Fuchs(2004)] Hohenwarter M, Fuchs K (2004) Combination of dynamic geometry, algebra and calculus in the software system geogebra. In: Computer Algebra Systems and Dynamic Geometry Systems in Mathematics Teaching Conference 2004, Pecs, Hungary

[Hull(2011)] Hull TC (2011) Solving cubics with creases: The work of Beloch and Lill. The American Mathematical Monthly 118(4):307–315

[Hulpke(1999)] Hulpke A (1999) Techniques for the computation of galois groups. In: Matzat B, Greuel GM, Hiss G (eds) Algorithmic Algebra and Number Theory, Springer Berlin Heidelberg, pp 65–77, DOI 10.1007/978-3-642-59932-3_4

[Ida et al.(2015)Ida, Ghourabi, and Takahashi] Ida T, Ghourabi F, Takahashi K (2015) Formalizing polygonal knot origami. Journal of Symbolic Computation 69(1):93–108

[Justin(1987)] Justin J (1987) Aspects mathmatiques du pliage de papier. L'Ouvert (47):1–14

[Kalkbrener(1993)] Kalkbrener M (1993) A generalized euclidean algorithm for computing triangular representations of algebraic varieties. J Symbolic Computation 15(2):143–167

[Kapur and Saxena(1995)] Kapur D, Saxena T (1995) Comparison of various multivariate resultant formulations. In: Levelt AHM (ed) Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation, ISSAC '95, Montreal, Canada, July 10-12, 1995, ACM, pp 187–194, DOI 10.1145/220346.220370, URL http://doi.acm.org/10.1145/220346.220370

[Laborde and Strasser(1990)] Laborde JM, Strasser R (1990) Cabri-géométre: A Microworld of Geometry for Guided Discovery Learning. Zentrablatt Für Didactic der Matematik 22(5):171–177

[Landau and Miller(1985)] Landau S, Miller GL (1985) Solvability by radicals is in polynomial time. J Comput Syst Sci 30(2):179–208, invited publication

[Lebesgue(1950)] Lebesgue H (1950) Leçons sur les constructions géométriques. Gauthier-Villars, Paris, in French, re-edition by Editions Jacques Gabay, France

[Lemaire et al.(2005)Lemaire, Maza, and Xie] Lemaire F, Maza MM, Xie Y (2005) The regularchains library in MAPLE. ACM SIGSAM Bulletin 39(3):96–97, DOI 10.1145/1113439.1113456, URL http://doi.acm.org/10.1145/1113439.1113456

[Marinković and Janičić(2012)] Marinković V, Janičić P (2012) Towards understanding triangle construction problems. In: Jeuring et al J (ed) Intelligent Computer Mathematics - CICM 2012, Springer, Lecture Notes in Computer Science, vol 7362

[Marinkovic et al.(2014)Marinkovic, Janicic, and Schreck] Marinkovic V, Janicic P, Schreck P (2014) Computer theorem proving for verifiable solving of geometric construction problems. In: Botana F, Quaresma P (eds) Automated Deduction in Geometry - 10th International Workshop, ADG 2014, Coimbra, Portugal, July 9-11, 2014, Revised Selected Papers, Springer, Lecture Notes in Computer Science, vol 9201, pp 72–93, DOI 10.1007/978-3-319-21362-0, URL http://dx.doi.org/10.1007/978-3-319-21362-0

[Mathis and Schreck(2016)] Mathis P, Schreck P (2016) Determining automatically compass and straightedge unconstructibility in triangles. In: Davenport JH, Ghourabi F (eds) 7th International Symposium on Symbolic Computation in Software Science, SCSS 2016, Tokyo, Japan, March 28-31, 2016, EasyChair, EPiC Series in Computing, vol 39, pp 130–142, URL http://www.easychair.org/publications/paper/262507

[Meyers(1996)] Meyers LF (1996) Update on William Wernick's „triangle constructions with three located points". Mathematics Magazine 69(1):46–49

[Narboux and Braun(2016)] Narboux J, Braun D (2016) Towards A Certified Version of the Encyclopedia of Triangle Centers. Mathematics in Computer Science 10(1):17, DOI 10.1007/s11786-016-0254-4, URL https://hal.inria.fr/hal-01174131

[Polya(1965)] Polya G (1965) Mathematical Discovery Volume II: On understanding, learning, and teaching problem solving. John Wiley and Sons Inc

[Scandura et al.(1974)Scandura, Durnin, and Wulfeck II] Scandura JM, Durnin JH, Wulfeck II WH (1974) Higher order rule characterization of heuristics for compass and straight edge constructions in geometry. Artificial Intelligence 5(2):149–183, DOI 10.1016/0004-3702(74)90028-9, URL http://www.sciencedirect.com/science/article/pii/0004370274900289

[Schreck(1993)] Schreck P (1993) Automatisation des constructions géométriques à la règle et au compas. PhD thesis

[Schreck(1994)] Schreck P (1994) Modélisation et implantation d'un système à base de connaissances géométriques. Revue d'intelligence artificielle 8(3):223–247

[Schreck and Mathis(2006)] Schreck P, Mathis P (2006) Geometrical constraint system decomposition: a multi-group approach. Int J Comput Geometry Appl 16(5-6):431–442, DOI 10.1142/S0218195906002129, URL https://doi.org/10.1142/S0218195906002129

[Schreck and Mathis(2016)] Schreck P, Mathis P (2016) Automatic constructibility checking of a corpus of geometric construction problems. Mathematics in Computer Science 10(1):41–56

[Schreck et al.(2016)Schreck, Marinkovic, and Janicic] Schreck P, Marinkovic V, Janicic P (2016) Constructibility classes for triangle location problems. Mathematics in Computer Science 10(1):27–39, DOI 10.1007/s11786-016-0255-3

[Song et al.(2017)Song, Wang, and Chen] Song D, Wang D, Chen X (2017) Retrieving geometric information from images: the case of hand-drawn diagrams. Data Min Knowl Discov 31(4):934–971, DOI 10.1007/s10618-017-0494-1, URL https://doi.org/10.1007/s10618-017-0494-1

[Stewart(2003)] Stewart I (2003) Galois Theory (third edition). Chapman Hall

[Wang(2016)] Wang D (2016) On the connection between ritt characteristic sets and buchberger-gröbner bases. Mathematics in Computer Science 10(4):479–492, DOI 10.1007/s11786-016-0279-8, URL https://doi.org/10.1007/s11786-016-0279-8

[Wernick(1982)] Wernick W (1982) Triangle constructions with three located points. Mathematics Magazine 55:227–230

[Wu(1984)] Wu WT (1984) Basic principles of mechanical theorem proving in elementary geometries. Journal of Symbolic Computation 4:207–235

[Wu(2008)] Wu WT (2008) Selected works of Wen-Tsun Wu. World Scientific