RC-(un)constructibility, proofs and constructions

Pascal Schreck

Université de Strasbourg - LSIIT, UMR CNRS 7005

12-12-12

Introduction

By opposition to other methods for solving geometric constraints, particularly in CAD, geometric constructions aim at computing exact solutions.

- This approach has some interest in CAD domain (and some drawbacks to be fair).
- The ingredients used are very similar to those used in proof in geometry.
- I take here the example of algebra by presenting Lebesgue's method.

Exact solution

Given a ∀∃ problem an exact solution is

- a symbolic object ...
- and a *proof* that it fulfills the specifications

Examples (outside of geometry)

- for all integer x, there is an integer y such that x+y=5
- for all list L, there is a sorted list L' containing exactly the same elements

A formal framework is needed

- to express the specification;
- to define the tools to perform the proof;
- (possibly) to construction the symbolic solution

RC-constructible numbers

- For the ancient Greeks, the set of the RC-constructible numbers + euclidean geometry was such a fundamental framework.
- Classical definition through the notions of points, lines and circles RC-constructible.
- But RC-constructible numbers can also be defined through constructible operations:
  - addition, subtraction;
  - multiplication, division;
  - square radical.
- There are famous unconstructibility issues.

Proofs

Different kinds of proof

- high level geometry
- logic and foundations
- combinatoric
- algebraic:Wu's method, Ritt-Wu principle.

In this talk, I will focus on the last point.

Wu's method roughly speaking

- translation from geometry to algebra
- "triangularization" of the system corresponding to the hypothesis
- successive pseudo-divisions of the goal by the hypothesis

Wu's method and algebra

- Roughly speaking, a theorem of the form $H \Rightarrow g$ is stated by
  - g belongs to $\sqrt{\langle H \rangle}$, or
  - $V(H) \subset V(g)$
- The point of the Ritt-Wu principle is precisely to characterize the Zero-set of a set of polynomials.
- It is then no surprising that the Ritt-Wu principle is also useful in (geometric) constraint satisfaction

In the following, I present a method mixing the Ritt-Wu's principle and the Lebesgue's method to exactly solve polynomial systems corresponding to RC-problems.

Lebesgue's method

Mathematical results

Definition (RC-constructible from O and I)

A real is RC-constructible *iff* it is a coordinate of a RC-constructible point in the plane.

Theorem (Wantzel 1837)

Each RC-constructible number is algebraic over $\mathbb{Q}$ *and its degree is equal to* 2^k *for some* $k \in \mathbb{N}$

Notes

- the converse is false: one of the roots of $X^4 - X - 1$ is not RC-constructible.
- this thm was used for famous impossibility theorems
- base of the theorem: "if $P \in \mathbb{Q}[X]$ with degree 3 has no rational root, then its roots are not RC-constructible"

Mathematical results (continued)

Theorem (Gallois ∼1870)

Let α be an algebraic number over $\mathbb{Q}$, $P(X)$ be its minimal polynomial and K be the splitting field of $P(X)$.
α is RC-constructible iff $[K : \mathbb{Q}] = 2^k$ for some $k \in \mathbb{N}$.

Notes

- Wantzel: RC-constructibility $\Rightarrow [R : \mathbb{Q}] = 2^l$ with $R =$ rupture field of P
- Gallois: RC-constructibility $\Leftrightarrow [K : \mathbb{Q}] = 2^k$
- Wantzel's result can prove unconstructibility, but not constructibility result.

Mathematical results (continued)

Galois's result and Lebesgue's method

- using Galois's result one can prove that α is RC-constructible *iff* it exists a sequence of fields $L_0, \ldots, L_k$ such that $L_0 = \mathbb{Q}$, $[L_{i+1} : L_i] = 2$ and $\alpha \in L_k$.
- Lebesgue compute the splitting field of an irreducible polynomial (with degree 2^k) by using a polynomial so called Galois's resolvent (with degree $(2^k)!$)

Theorem (Chen-Carrayol 1992)

Let α be an algebraic number over $\mathbb{Q}$, α is RC-constructible iff there is a sequence of fields $L_0, \ldots, L_k$ such that $L_0 = \mathbb{Q}$, $[L_{i+1} : L_i] = 2$ and $L_k = \mathbb{Q}[\alpha]$.
Then the minimal polynomial of α is decomposable on L_1.

About computability

Definition (computable filed)

A field $(K, +, *)$ is computable if the operations $+, -, *$ and $/$ are computable

Definition (RP-computability)

A field $(K, +, *)$ is RP-computable if it is computable and there is an algorithm to compute the roots in K for every polynomials $P \in K[X]$.

Examples

- finite fields
- $\mathbb{Q}$

Factorization

Theorem

A field K is RP-computable iff there is a factorization algorithm in $K[X]$.

Sketch of the proof: ($\Leftarrow$ is obvious)

* $\Rightarrow$:

Let $X^k + a_1X^{k-1} + \dots a_{k_1}X + a_k$ be a factor of $P(X)$. By euclidean division we have:

$$P(X) = Q(X)(X^k + a_1X^{k-1} + \dots a_{k_1}X + a_k) + R(X)$$

with $R(X) = 0$ and each coeff r_i of R belongs to $K[a_1, \dots a_k]$.

$$\begin{cases} r_{k-1}(a_1, \dots, a_k) = 0 \\ \dots \\ r_0(a_1, \dots, a_k) = 0 \end{cases} \text{giving} \quad \begin{cases} r'_{k-1}(a_1) = 0 \\ \dots \\ r'_0(a_1, \dots, a_k) = 0 \end{cases}$$

Factorization (continued)

Notes

- Triangularization by computing Ritt-Wu characteristic sets, or euclidean division in some rational field, or using Groebner basis.
- solving the triangular system by using the algorithm for computing roots of polynomials in $K[X]$.
- of course, there are better algorithms to factorize polynomials (Kronecker, Berlekamp, Cantor-Zassenhaus, Wang for algebraic extensions of $\mathbb{Q}$)

RP-computability and field extension

Theorem

Let $K \subset F$ be a field extension and μ be an element of F. If K is RP-computable, $K(\mu)$ is RP-computable too.

Corollary

With the same notations, there is a factorization algorithm for $K(\mu)[X]$

Recall

Theorem
α is RC-constructible iff there is a sequence $\alpha 1, \ldots \alpha_k = \alpha$ such that $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\alpha_{i+1}, \ldots \alpha_1) : \mathbb{Q}(\alpha_i, \ldots \alpha_1] = 2$

Theorem
Let $P(X)$ be an irreducible polynomial in $K[X]$ (K being an algebraic extension of $\mathbb{Q}$); if $P(X) = 0$ is solvable using square roots then there is some $r \in K$ such that $P(X)$ is decomposable on $K(\sqrt{r})$.

Use

Let $P(X)$ be an irreducible polynomial on K, let's try to find r and to factorize P.

If $Q(X)$ is such a factor, we have ($m_i \in K, r \in K$):

$$Q(X) = X^k + m_1 X^{k-1} + \ldots + m_k + \sqrt{r}(m_{k+1}X^{k-1} + \ldots + m_{2k})$$

by euclidean division: $P(X) = Q(X)T(X) + R(X)$ with

$$R(X) = (A_0(m_1, \ldots, m_{2k}, r) + \sqrt{r}B_0(m_1, \ldots, m_{2k}, r))X^{k-1} +$$

$$\ldots + A_{k-1}(m_1, \ldots, m_{2k}, r) + \sqrt{r}B_{k-1}(m_1, \ldots, m_{2k}, r)$$

where each A_i and B_j belong to $K[m_1, \ldots, m_{2k}, r]$.
Moreover $R(X)$ should be the null polynomial.

Use (continued)

This leads to solve the algebraic system (S_0):

$$\begin{cases} A_0(m_1, \ldots, m_{2k}, r) = 0 \\ \ldots \\ A_{k-1}(m_1, \ldots, m_{2k}, r) = 0 \\ B_0(m_1, \ldots, m_{2k}, r) = 0 \\ \ldots \\ B_{k-1}(m_1, \ldots, m_{2k}, r) = 0 \\ (m_{k+1} - 1)(m_{k+2} - 1) \ldots (m_{2k} - 1) = 0 \end{cases}$$

where the unknowns $m_1, \ldots, m_{2k}$ et r are to be solved in K. Solving S_0 uses triangularization and the algorithm for finding roots in K.

Use (continued)

- If there is no solution, $P(X)$ is not decomposable and the process ends.
- If there is a solution for S_0, when polynomial $P(X)$ can be decomposed, and the process recursively goes on on each factor taking $\mathbb{Q}(\sqrt{r})$ for K.
- at the end, either polynomial is totally split (and we have a characterization of its splitting field), or the polynomial is not decomposable.

Ritt-Wu's principle

Revealing the cheater

I was very imprecise when talking about Wu's method in geometric proof or triangulation.

What I said

- Roughly speaking, a theorem of the form $H \Rightarrow g$ is stated by
  - g belongs to $\sqrt{\langle H \rangle}$, or
  - $V(H) \subset V(g)$

Actually (Chou)

For most geometry theorems, some hypothesis are des-equality specifying degenerate cases:

- $\forall y \in E. h_1 = 0 \wedge \ldots h_n = 0 \wedge s_1 \neq 0 \ldots s_k \neq 0 \Rightarrow g = 0$

Revealing the cheater (continued)

What I said

Triangularization by computing Ritt-Wu characteristic sets.

More precisely (Ritt-Wu and Chou)

Given a finite set of polynomials $\{h_1, \ldots h_m\}$, its zero-set can be decomposed into irreducible components $(V(P_1^*) \cup \ldots V(P_c^*)) \cup (V(P_1^+) \ldots V(P_e^+)) \cup (V(P_1) \cup \ldots V(P_t))$ (some of them correspond to degenerate cases)

Consequences

- It leads to a more complex notion of the validity of a theorem: it can be true in one component and false on another one
- when one want to solve a construction system, triangularization cannot be just the simple Chou method and, moreover, it leads to more than one irreducible triangular system.

Examples

A successful resolution (1) (Chen)

Statement. Construct a triangle given the length p_1 of side BC, and the lengths of the altitudes from A (p_2) and B (p_3).
Parametrization: $B(0,0), C(p_1,0), A(x_1,x_2)$. We have the equations:
$f_1 : x_2^2 - p_2^2 = 0$
$f_2 : p_1^2 x_2^2 - p_3^2((x_1 - p_1)^2 + x_2^2)$

We get 2 irreducible characteristic sets:
$g_1 = 2p_3^2 x_1 p_1 - p_3^2 x_1^2 - p_3^2 p_1^2 - p_2^2 p_3^2$
$g_2(g_3) = x_2 \pm p_2$

A successful resolution (1) continued

it leads to four solutions (2 up to symmetries):

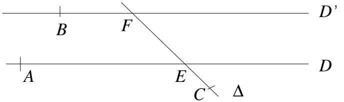
$$x_1 = -\frac{-2p_3^2 p_1 \pm 2p_2 p_3 \sqrt{p_1^2 - p_3^2}}{2p_3^2},\ x_2 = p_2$$

$$x_1 = -\frac{-2p_3^2 p_1 \pm 2p_2 p_3 \sqrt{p_1^2 - p_3^2}}{2p_3^2},\ x_2 = -p_2$$

The straightedge and compass construction can be automatically deduced from this ... but it is not very interesting.

A successful resolution (2) continued

Statement. Given two parallel lines D and D', and three points: A on D, B on D' and C. Construct a line Δ passing through C and cutting D in E and D' in F such that $AE + BF$ equals the given length p_1.



$B(0,0), D' = Ox$
$A(p_2,p_3), C(p_4,p_5), E(x_1,x_2), F(x_3,x_4)$

We get:

$f_1 : x_4 = 0$
$f_2 : x_2 - p_3 = 0$
$f_3 : (x_2 - p_5)(x_3 - p_4) - (x_1 - p_4)(x_4 - p_5) = 0$
$f_4 : \left((x_1 - p_2)^2 + (x_2 - p_3)^2 + x_3^2 + x_4^2 - p_1^2\right)^2 - 4(x_1 - p_2)^2$
$\quad -4(x_2 - p_3)^2 - 4x_3^2 - 4x_4^2 = 0$

A successful resolution (2) continued

We have only one irreducible component, and the solving gives $x_1 = s_1 + s_2$, avec
$s_1 = \sqrt{\frac{u}{v}}$, $s_2 = \frac{-q}{r}$, et

$$u = 8p_3^4 + 8p_3^4\sqrt{1+p_1^2} - 4p_3^4p_4^2 + 4p_3^4p_1^2 + 8p_5p_3^3p_4p_2 - 32p_5p_3^3 + 8p_3^3p_4^2p_5 - 32p_3^3p_5\sqrt{1+p_1^2} - 16p_5p_3^3p_1^2 - 4p_5^2p_2^2 - 16p_5^2p_3^2p_4p_2 + 56p_5^2p_3^2 + 28p_5^2p_3^2p_1^2 + 56p_3^2p_5^2\sqrt{1+p_1^2} - 4p_3^2p_4^2p_5^2 + 8p_5^3p_2^2p_3 + 8p_5^3p_3p_4p_2 - 48p_5^3p_3 - 24p_5^3p_3p_1^2 - 48p_3p_5^3\sqrt{1+p_1^2} + 16p_5^4 8p_5^4p_1^2 + 16p_5^4\sqrt{1+p_1^2} - 4p_5^4p_2^2,$$

$$v = 2p_3^2 - 4p_3p_5 + 4p_5^2$$

$$q = -4p_4p_3^3p_5 - 28p_5^2p_2p_3^2 + 24p_5^3p_2p_3 - 8p_4p_3p_5^3 + 8p_4p_3^2p_5^2 + 16p_5p_2p_3^3 - 8p_5^4p_2 - 4p_2p_3^4$$

$$r = 16p_5^4 - 16p_5p_3^3 + 4p_3^4 - 32p_5^3p_3 + 32p_5^2p_3^2$$

A proof of unconstructibility

I just checked problem #90 of Wernick list (I thought that it had no status according to Meyer, but it is known as unsolvable after Vesna and Predrag paper)

In this problem, we know incenter I, midpoints M_a and M_b. Putting I at $(0,0)$ and M_a at $(1,0)$ we get the two equations:

$$f_1 : ((2*yA-2*yMb)^2+(2*xA-2*xMb)^2)*(2*xA*yMb-(2*xMb-2)*yA)^2$$

$$-(-xA*(2*yMb-2*yA)-(2*xA-2*xMb)*yA)^2*(4*yMb^2+(2*xMb-2)^2)=0$$

$$f_2 : (4*(yA-2*yMb)^2+(2*(-2*xMb+xA+2)-2)^2)*(-2*(-2*xMb+xA+2)*yMb-(2-2*xMb)*(yA-2*yMb))^2$$

$$-(2*(-2*xMb+xA+2)*(yA-2*yMb)-(2*(-2*xMb+xA+2)-2)*(yA-2*yMb))^2*(4*yMb^2+(2*xMb-2)^2)=0$$

Each of degree 4 with respect to yA.
Trying eliminate yA by simple Chou 's algorithm, we get only one equation!
Either the triangularization fails, or the status of the problem is L

A proof of unconstructibility (continued)

In fact, there is a common factor to the two equation corresponding to the degenerate case. Using the `factor` command of Maxima, we have:

$f_1 : (xMb - 1) * yA^3 + (-2 * xMb - xA + 1) * yMb * yA^2$
$+(2*xA*yMb^2 - 2*xA*xMb^2 + (xA^2 + 2*xA)*xMb - xA^2)*yA$
$+(2 * xA^2 * xMb - xA^3 - xA^2) * yMb = 0$

and

$f_2 : (-xMb + 1) * yA^3 + (4 * xMb + xA - 3) * yMb * yA^2$
$+((-4 * xMb - 4 * xA) * yMb^2 - 4 * xMb^3 + (4 * xA + 8) *$
$xMb^2 + (-xA^2 - 6 * xA - 4) * xMb + xA^2 + 2 * xA) * yA$
$+(4 * xA + 4) * yMb^3 + ((4 * xA + 4) * xMb^2 + (-4 * xA^2 -$
$8 * xA - 8) * xMb + xA^3 + 3 * xA^2 + 4 * xA + 4) * yMb = 0$

by simple triangularization (degree 5 wrt xA

$$((-32*xMb+32)*yMb^9+(-96*xMb^3+288*xMb^2-288*xMb+96)*yMb^7+(-96*xMb^5+480*xMb^4-960*xMb^3+960*xMb^2-480*xMb+96)*yMb^5+(-32*xMb^7+224*xMb^6-672*xMb^5+1120*xMb^4-1120*xMb^3+672*xMb^2-224*xMb+32)*yMb^3)*xA^5+((256*xMb^2-608*xMb+352)*yMb^9+(768*xMb^4-3072*xMb^3+4608*xMb^2-3072*xMb+768)*yMb^7+(768*xMb^6-4320*xMb^5+10080*xMb^4-12480*xMb^3+8640*xMb^2-3168*xMb+480)*yMb^5+(256*xMb^8-1856*xMb^7+5824*xMb^6-10304*xMb^5+11200*xMb^4-7616*xMb^3+3136*xMb^2-704*xMb+64)*yMb^3)*xA^4+((-768*xMb^3+2688*xMb^2-3072*xMb+1152)*yMb^9+(-2304*xMb^5+11136*xMb^4-21888*xMb^3+21888*xMb^2-11136*xMb+2304)*yMb^7+(-2304*xMb^7+14208*xMb^6-37632*xMb^5+55680*xMb^4-49920*xMb^3+27264*xMb^2-8448*xMb+1152)*yMb^5+(-768*xMb^9+5760*xMb^8-18816*xMb^7+34944*xMb^6-40320*xMb^5+29568*xMb^4-13440*xMb^3+3456*xMb^2-384*xMb)*yMb^3)*xA^3+((1024*xMb^4-4608*xMb^3+7808*xMb^2-5760*xMb+1536)*yMb^9+(3072*xMb^6-17152*xMb^5+41472*xMb^4-55296*xMb^3+42496*xMb^2-17664*xMb+3072)*yMb^7+(3072*xMb^8-20480*xMb^7+60544*xMb^6-104576*xMb^5+116480*xMb^4-86272*xMb^3+41600*xMb^2-11904*xMb+1536)*yMb^5+(1024*xMb^1 0-7936*xMb^9+26880*xMb^8-51968*xMb^7+62720*xMb^6-48384*xMb^5+23296*xMb^4-6400*xMb^3+768*xMb^2)*yMb^3)*xA^2+((-128*xMb+128)*yMb^1 1+(-512*xMb^5+3072*xMb^4-7552*xMb^3+9088*xMb^2-5248*xMb+1152)*yMb^9+(-1536*xMb^7+10240*xMb^6-31104*xMb^5+54656*xMb^4-58624*xMb^3+37632*xMb^2-13184*xMb+1920)*yMb^7+(-1536*xMb^9+11264*xMb^8-38016*xMb^7+78464*xMb^6-109696*xMb^5+$$

Simplification

We can take the specific example with $Mb(-2,3)$ since we want to prove the non-RC-constructibility of triangle ABC. We get, after simplification

P :

$$2*xA^5+45*xA^4+372*xA^3+1368*xA^2+2160*xA+972=0$$

Either P is irreducible (and then we have proved RC-unconstructibility since degree of xA is not a power of 2) or we can decompose it: since it has no rational root (I checked) the factors has resp. degree 2 and 3.

Actually, Maxima is powerful enough to prove that P is irreducible. But we can apply the Lebesgue's method since it was the goal of the speech.

(once again, my apologies, I had no time to take another example).

Preliminary

So, $P(X)$ has no root in $\mathbb{Q}$. We consider all the cases:

1. $P(X)$ is irreducible (then it's ok)
2. $P(X)$ is decomposable: $P = QR$ with $deg(Q) = 3$ and $deg(R) = 2$. and we have to consider either Q or R as the minimal polynomial of xA.
   - $Q(X)$ is irreducible (since $P(X)$ has no root in $\mathbb{Q}$), so if Q is the minimal polynomial of xA, its ok
   - R is irreducible, so applying the Lebesgue's method, we have to find a root in $\mathbb{Q}$.

Replacement $xA = a + \sqrt{b}$

$\sqrt{b} * (2 * b^2 + (20 * a^2 + 180 * a + 372) * b + 10 * a^4 + 180 * a^3 + 1116 * a^2 + 2736 * a + 2160)$
$+(10 * a + 45) * b^2 + (20 * a^3 + 270 * a^2 + 1116 * a + 1368) * b + 2 * a^5 + 45 * a^4 + 372 * a^3 + 1368 * a^2 + 2160 * a + 972$
$= 0$

Then, we should have:

$2 * b^2 + (20 * a^2 + 180 * a + 372) * b + 10 * a^4 + 180 * a^3 + 1116 * a^2 + 2736 * a + 2160 = 0$

and:

$(10 * a + 45) * b^2 + (20 * a^3 + 270 * a^2 + 1116 * a + 1368) * b + 2 * a^5 + 45 * a^4 + 372 * a^3 + 1368 * a^2 + 2160 * a + 972 = 0$

continued again

Using triangularization and eliminating b, we get:
$256 * a^10 + 11520 * a^9 + 230112 * a^8 + 2685168 * a^7 + 20253753 * a^6 + 103083246 * a^5 + 358125840 * a^4 + 837646920 * a^3 + 1261104147 * a^2 + 1102911390 * a + 425668932 = 0$

to solve in $\mathbb{Q}$. We consider all the possibilities $\frac{p}{q}$:
with q dividing $256 = 2^8$ (or 2^6)
and p dividing $425668932 = 2^2 * 3^7 * 13 * 19 * 197$ (or $3^7 * 13 * 19 * 197$

It is tedious but easy to verify this.

Some questions?