About the Lebesgue method

Pascal Schreck

October 15, 2003

Abstract

This is a sketch of my talk about the Lebesgue method for deciding if an equation is solvable using only square radicals, and then for solving it exactly.

1 Introduction

When one have to solve equations, in particular geometric constraints, two objectives can be pursued : finding the exact solutions, or, finding numerical results which are approximations of the solutions.

Usually, the approximating methods are more general and faster than exact methods, and they can be used in a lot of situations. Sometimes, however, these qualities do not make up for the drawbacks that may be related. This is the case in educational domain where the method used to find the solutions can be as important as the result itself. The situation occurs as well when the problems are poorly conditioned and when the quality of the found results is questionable.

Since our (small) team dealt with formal methods in software engineering for geometric modeling, we got interested in studying symbolic methods for geometric constraints solving. So, we studied geometric constructions firstly with a geometrical and logical point of view, and, secondly following the algebraic way. For the second point, we used a method proposed by Lebesgue in order to solve, if possible, an irreducible univariate polynomial using only square radicals: this method was simplified and implemented in Maple by Guoting Chen in the earlier 90' (note that this method seems different to the one described by X-S Gao and S-C Chou). This work is the main subject of my talk.

2 Classical results

First, let me recall some classical results about geometry and rule and compass constructions (RC-constructions in short).

It is well known that there are some insoluble problems using only rule and compass (such as the angle trisection and squaring the circle), but it is not so easy to detect if a construction problem is RC-constructible or not.
For instance, the Cramer-Castillon problem (which is "given Γ, A, B and C, construct M, N and P on Γ such that $A \in (MN)$, $B \in (NP)$ and $C \in (MP)$")

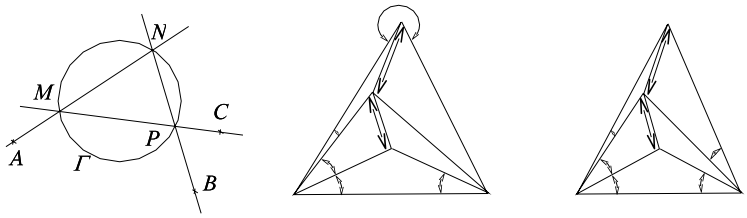

Figure 1: Three problems a) Cramer-Castillon problem, b) and c) length and angle constrained figures

is RC-constructible. One of the subfigures b) and c) on Fig. 1 is not RC-constructible: it is not so easy to guess which one and why.

In year 1837, P. L. Wantzel gave the well-known property of RC-constructibility of real numbers :

> **Theorem 2.1** Each number which is RC-constructible from points (0,0) and (1,0) is algebraic over $\mathbb{Q}$ and its degree is equal to 2^k for some $k \in \mathbb{N}$.

This result can be applied to the trisection problem. Note that the reverse is false, for instance

$$P(X) = X^4 - X - 1$$

is the minimal polynomial of an algebraic number which is not RC-constructible. In fact, the Galois theory (1832) was used to prove the following well-known characterization of RC-constructible numbers :

> **Theorem 2.2** Let α be a real number algebraic over $\mathbb{Q}$, $P(X)$ be its minimal polynomial and K be the splitting field of $P(X)$. α is RC-constructible if and only if $[K : \mathbb{Q}] = 2^k$ for some $k \in \mathbb{N}$.

Note that these theorems are still true in the general case, where parameters are given (that is : instead of $\mathbb{Q}$, the field of rational fractions $\mathbb{Q}(t_1, \ldots, t_p)$ is considered as the base field).

So, to prove that a problem is RC-constructible, we have in some sense to compute the corresponding splitting field. In the early 40's Lebesgue gave a method using the so-called "résolvante de Galois" which is a polynomial with a high degree, but G. Chen gave another characterization of the RC-constructible number which is more acurate than the Wantzel property and more usefull than theorem 2.2 (the proof of this theorem was done by G. Chen and H. Carrayol):

> **Theorem 2.3** If α is RC-constructible number from points (0,0) and (1,0), then there is a finite sequence of fields $K_0, \ldots K_n$ such that:
>
> - $K_0 = \mathbb{Q}$

- $K_n = \mathbb{Q}(\alpha)$
- $[K_{i+1} : K_i] = 2$

.

The proof of this theorem needs some elements of Galois theory and technics of group theory. The main ingredient, apart from the Galois theorem, comes from the following lemma:

Lemma 2.4 Let G be a 2-group, and $H \subset G$ a sub-group of G. There is a sequence of groups $H_0, \ldots, H_n$ such that:

- $H_0 = H$
- $H_n = G$
- $H_i \subset H_{i+1}$ and $|H_{i+1}/H_i| = 2$

Theorem 2.3 leads to a simplification of Lebesgue's method which becomes expressible using only elementary mathematics. This is the subject of the next section.

3 Lebesgue method

3.1 Preliminaries

In the following, we consider a "computable" field $\mathbb{K}$, i.e. a field where there are algorithms to perform the usual arithmetic operations in $\mathbb{K}$. We say that $\mathbb{K}$ is RP-computable, if it is computable and if there is an algorithm to compute all the roots in $\mathbb{K}$ for all given polynomials $P(X)$ in $\mathbb{K}[X]$. For instance $\mathbb{Q}$ is RP-computable. Then, we easily have:

Theorem 3.1 A field $\mathbb{K}$ is RP-computable if and only if there is a factorization algorithm for the ring $\mathbb{K}[X]$.

Proof:
The "if" part is self-evident since a factorization algorithm allow to find the factors of degree 1.
The "only if" demonstration is an interesting introduction to the Lebesgue method: Let P be a polynomial of $\mathbb{K}[X]$. Finding the factors of degree 1 is equivalent to finding the roots of P.

Suppose now that P have a factor of degree 2, say $X^2+\alpha X+\beta$. By Euclidean division, we have:

$$P(X) = Q(X)(X^2 + \alpha X + \beta) + R(X)$$

with $R(X)$ a polynomial of $\mathbb{K}[\alpha, \beta][X]$ with degree 1. Let $R(X) = A(\alpha, \beta)X + B(\alpha, \beta)$, since $R = 0$, we must have:

$$\begin{cases} A(\alpha, \beta) = 0 \\ B(\alpha, \beta) = 0 \end{cases}$$

By using pseudo division, this algebraic system can be put under triangular form:

$$\begin{cases} A'(\alpha) = 0 \\ B'(\alpha, \beta) = 0 \end{cases}$$

which, in turn, can be solved in $\mathbb{K}$ since $\mathbb{K}$ is RP-solvable.

Higher degree factors can be treated in the same way. □

The following usefull theorem is also easy to obtain.

Theorem 3.2 Let $\mathbb{K} \subset \mathbb{F}$ be a field extension and μ be an element of $\mathbb{F}$. If $\mathbb{K}$ is RP-computable, so is $\mathbb{K}(\mu)$.

Two cases must be considered : even μ is algebraic or μ is transcendantal.
Transcendantal case:
Without loss of generality, we can consider a polynomial $f \in \mathbb{K}[\mu][X]$ (instead of $f \in \mathbb{K}(\mu)[X]$). Let us write: $f(X) = \alpha_n X^n + \ldots \alpha_1 X + \alpha_0$ where α_i are in $\mathbb{K}[\mu]$. We use, once again, the fact that $\mathbb{K}[\mu]$ is factorial: each root of f can be written $x_0 = p/q$ (with p and q in $\mathbb{K}[\mu]$ and relatively prime). Then p divides α_0 and q divides α_n. Since $\mathbb{K}$ is RP-solvable, there is a factorization algorithm for $\mathbb{K}[\mu]$: this algorithme is used in order to find the factors of α_n and the ones of α_0.

Algebraic case:
We consider that μ is given by its minimal polynomial P of degree k. Let $f(X) = \alpha_n X^n + \ldots \alpha_1 X + \alpha_0$ be a polynomial of $\mathbb{K}(\mu)[X]$ (that is, each α_i is in $\mathbb{K}(\mu)$ and $\mathbb{K}(\mu) = \mathbb{K}[\mu]$ since μ is algebraic). So, each α_i can be written $\alpha_i = a_{i,k-1}\mu^{k-1} + \ldots + a_{i,0}$ where each $a_{i,j}$ is in $\mathbb{K}$. (In practice, one can put a rational fraction $\frac{c_n\mu^n+\ldots+c_0}{d_m\mu^m+\ldots+d_0}$ under the form $a_{k-1}\mu^{k-1} + \ldots + a_0$ by using Euclidean division by P and Bezout relation between P and the denominator of the fraction).

In the same way, each solution x_0 for $f(X) = 0$ which is in $\mathbb{K}[\mu]$ can be written $x_0 = b_{k-1}\mu^{k-1} + \ldots b_0$. By expanding $f(x_0)$ with respect of μ and by reducing the result with the help of P, we obtain:

$$f(x_0) = \beta_{k-1}\mu^{k-1} + \ldots \beta_0 = 0$$

where β_i is a polynomial of $\mathbb{K}[b_{k-1}, \ldots b_0]$. Since the set $\{\mu^{k-1}, \ldots, \mu, 1\}$ is linearly independent, each β_i must be nul:

$$\begin{cases} \beta_{k-1}(b_{k-1}, \ldots, b_0) = 0 \\ \ldots \\ \beta_0(b_{k-1}, \ldots, b_0) = 0 \end{cases}$$

This system can be solved, *in* $\mathbb{K}$, using the same method as above.

3.2 Lebesgue method

The problem of RC-constructibility of a number α defined by an irreducible polynomial $P(X) \in \mathbb{K}[X]$ consists in finding some numbers $r_1, \ldots r_n$ such that $r_i \in \mathbb{K}(\sqrt{r_1}, \ldots \sqrt{r_{i-1}})$ and $\mathbb{K}(\sqrt{r_1}, \ldots \sqrt{r_{i-1}}, \sqrt{r_n})$ is the splitting field of $P(X)$. Lebesgue used the so-called "résolvante de Galois". But the method can be simplified considering the following theorem:

Theorem 3.3 Let $P(X)$ be an irreducible polynomial over $\mathbb{K}$. If $P(X) = 0$ is solvable using only square radicals, then there is $r \in \mathbb{K}$ such that $P(x)$ is reducible over $\mathbb{K}(\sqrt{r})$

Proof.
Let x_0 be a root of P and n be the degree of P. Since x_0 is square radicals expressible, we have $\mathbb{K}(x_0) = \mathbb{K}(\sqrt{r_1}, \ldots \sqrt{r_{i-1}}, \sqrt{r_m})$ for some r_j (with $r_j \in \mathbb{K}(\sqrt{r_1}, \ldots \sqrt{r_{j-1}})$, see thm. 2.3). So, we have:

$$\mathbb{K} \subseteq \mathbb{K}(\sqrt{r_1}) \subseteq \mathbb{K}(x_0)$$

with $\sqrt{r_1} \notin \mathbb{K}$ and then $[\mathbb{K}(x_0) : \mathbb{K}(\sqrt{r_1})] = n/2$. Since $n/2 < n$, P is not irreducible over $\mathbb{K}(\sqrt{r_1})$. □

Now, we can use this theorem as follows:

Let $P(X) = X^n + a_1 X^{n-1} \ldots + a_{n-1}$ be an irreducible polynomial over $\mathbb{K}$, a factor of $P(X)$ in $\mathbb{K}(\sqrt{r})[X]$ can be written: $Q(X) = X^k + m_1 X^{k-1} \ldots m_k + \sqrt{r}(m_{k+1} X^{n-1} + \ldots + m_{2k})$. Doing the euclidean division of P by Q, we have:

$$P(X) = Q(X) * T(X) + R(X)$$

where

$$\begin{aligned} R(X) = \quad & (A_0(m_1, \ldots, m_{2k}, r) + \sqrt{r} B_0(m_1, \ldots, m_{2k}, r)) X^{k-1} + \\ & \ldots \\ & + A_{k-1}(m_1, \ldots, m_{2k}, r) + \sqrt{r} B_{k-1}(m_1, \ldots, m_{2k}, r) \end{aligned}$$

with $A_i(m_1, \ldots, m_{2k}, r) \in \mathbb{K}[Y_1, \ldots Y_{2k}, Y_{2k+1}]$ and $B_i(m_1, \ldots, m_{2k}, r) \in \mathbb{K}[Y_1, \ldots Y_{2k}, Y_{2k+1}]$ Since there is an integer $i :\ k+1 \leqslant i \leqslant 2k$ such that $m_i \neq 0$, we can add the equation : $C(m_{k+1}, \ldots m_{2k}) = (m_{k+1} - 1)(m_{k+2} - 1) \ldots (m_{2k} - 1) = 0$. So, we have to solve the system :

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

where the unknowns $m_1, \ldots, m_{2k}$ and r are in $\mathbb{K}$.

This can be done:

- first, by a triangulation using Wu-Ritt algorithm (we have a factorization algorithm in $\mathbb{K}[X]$, then we can obtain irreducible triangular systems),
- second, by solving the resulting equations in $\mathbb{K}$ which is RP-computable.

So, we have to try all the possible factors for $P(X)$: if there is no factor, then $P(X)$ is not solvable using square radicals, otherwise we have to continue with each factor considering the field $\mathbb{K}(\sqrt{(r)})$

3.3 Examples

I will present some experiments with this method during my talk.

4 Conclusion and discussion

I have presented the Lebesgue method which permits to solve, if it is possible, algebraic equations using only square radicals. This method was implemented in Maple and experimented by G. Chen. It is not usable apart from small problems since it has at least exponential complexity. But, it gives a decision procedure for a large class of problems. Some improvements to the method could be realized considering the questions in the next subsections.

4.1 About the feasibility of calculi

To use the Lebesgue method, we have sometimes to decide if two constructible numbers are equal or not, and if some algebraic expressions of numbers are positive or not. There are some decision procedures for the equality problem (such a procedure was described by M. Mignotte in the 70'), and the cylindric decomposition method could be used to address the second question.

4.2 About rule and compass, and origami

The rule and compass constructions give a kind of standard for the domain of geometric constructions (and geometric constraints solving ...) since they define a large domain of difficult problems. Conversely, the angle trisection seems to be a "discrediting" counter-example: it appears as a simple problem but it is RC-unsolvable. Adding the possibility to do some foldings defines a greater class of constructions which is called origami constructions. In this framework, one can solve the trisection angle problem. More generally, one can prove that origami constructions correspond to equations solvable using only square and cubic radicals (so, the equations of degrees 2, 3 and 4 are all origami-solvable). The interesting thing is that the Lebesgue method can be improved to give a decision procedure to origami-constructibility.

4.3 About decidability of rule and compass constructions

First, note that A.Tarski excludes the rule and compass constructions from his elementary geometry. In fact, it is well-known in logic that the general rule and compass construction problem is *not expressible* within a first order logical framework.

The Lebesgue procedure shows that there is a decision procedure for RC-constructibility concerning the problems that are translatable into algebraic equations. But, in some domain such as in educational domain, there are problems which are not translatable into algebraic equations. The question is : given a geometric universe including rule and compass constructions, is there an algorithm for deciding if some problem is RC-constructible or not, without going out the geometric universe ?