Towards automated readable proofs of ruler and compass constructions

Vesna Marinković, Tijana Šukilović, Filip Marić

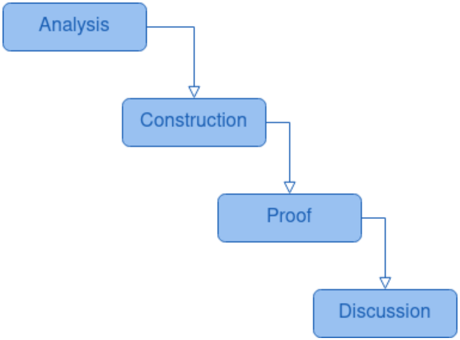
Faculty of Mathematics, University of Belgrade, Serbia

ADG 21. 9. 2024.

Solving ruler and compass construction problems

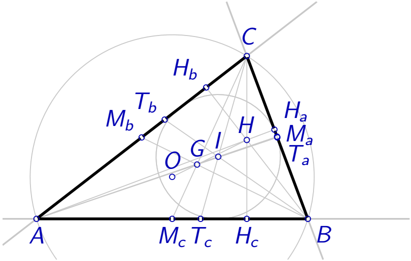
- One of the most studied problems in mathematical education
- Task: to describe a construction of geometrical figure which satisfies given set of constraints
  " construct $\triangle ABC$ given α, β and $|AB|$"
- Constructions are procedures
- Some instances are unsolvable (e.g. angle trisection)

Phases in solving construction problems



ArgoTriCS

- ArgoTriCS – system for automated solving of location construction problems from the given corpus (authors: V. Marinković, P. Janičić)
- Task of location triangle construction problem is to construct $\triangle ABC$ if locations of three significant points in the triangle are given
- Tool was tested on Wernick's corpus



- Requires background geometrical knowledge

ArgoTriCS

1. *Using the point A and the point H_a, construct a line h_a (rule W02);*

   % DET: points A and H_a are not the same

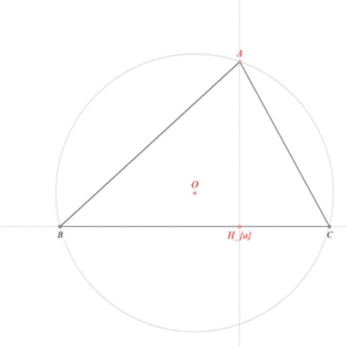
2. *Using the point A and the point O, construct a circle k(O,C) (rule W06);*

   % NDG: points A and O are not the same

3. *Using the point H_a and the line h_a, construct a line a (rule W10a);*

4. *Using the circle k(O,C) and the line a, construct a point C and a point B (rule W04);*

   % NDG: line a and circle k(O,C) intersect



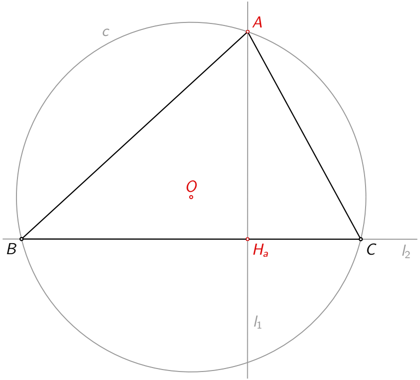
- Exports informal textual description of construction, as well as formal description of construction in GCLC and JSON format
- Enables generation of dynamic illustrations
- Constructions are proved correct using algebraic and semi-algebraic methods

The goal of research

- Existing systems for solving RC-constructions DO NOT provide classical, human-readable synthetic correctness proofs
- In current work we propose first steps towards obtaining readable, but also formal correctness proofs of automatically generated RC-constructions
- Synergy of various tools: triangle construction solver ArgoTriCS, FOL provers, coherent logic provers and interactive theorem provers

Example 1 – construction phase

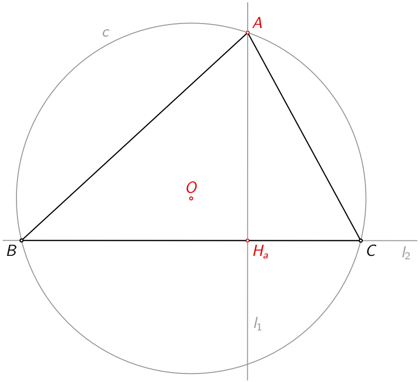
- Task: Construct $\triangle ABC$ given its vertex A, circumcenter O, and altitude foot H_a



1. Construct the line $l_1 = AH_a$
2. Construct the line $l_2 \colon l_2 \perp l_1$ and $H_a \in l_2$
3. Construct the circle c centered at O containing A
4. Let B and C be the intersections of the line l_2 and the circle c

Example 1 – proof phase

- Task: Prove that A is the vertex of the constructed triangle ABC, that H_a is its altitude foot and that O is its circumcenter



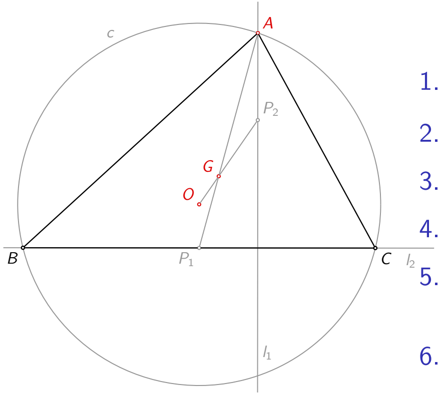
1. c contains vertices A, B, and C, so it must be the circumcircle of $\triangle ABC$
2. O is the center of c, so it must be the circumcenter of $\triangle ABC$
3. l_2 contains the vertices B and C, so it must be equal to side a of $\triangle ABC$
4. l_1 contains A and is perpendicular to $l_2 = a$, so it must be equal to altitude h_a
5. H_a belongs both to $l_2 = a$ and $l_1 = h_a$, so it must be the altitude foot

Conclusions following from Example 1

- The previous correctness proof follows quite directly from the analysis: it just reverses the chain of deduction steps
- The proof relies on several uniqueness lemmas
- One could conclude that it is always easy like this, however...
- ... in some cases the proof is quite different from the analysis

Example 2 – construction phase

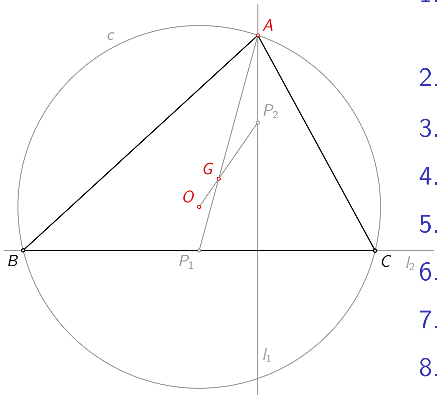
- Task: Construct $\triangle ABC$ given its vertex A, circumcenter O and centroid G



1. Construct the point $P_1 : \overrightarrow{AG} : \overrightarrow{AP_1} = 2 : 3$
2. Construct the point $P_2 : \overrightarrow{OG} : \overrightarrow{OP_2} = 1 : 3$
3. Construct the line $l_1 = AP_2$
4. Construct the line $l_2 : l_2 \perp l_1$ and $P_1 \in l_2$
5. Construct the circle c centered at O containing A
6. Let B and C be the intersections of the line l_2 and the circle c

Example 2 – proof phase

- Task: Prove that A is the vertex of the constructed triangle ABC, that G is its centroid and that O is its circumcenter



1. ... similarly to earlier we get that O is the circumcenter of $\triangle ABC$, $l_2 = a$ and $l_1 = h_a$
2. $\overrightarrow{OG} : \overrightarrow{OP_2} = 1 : 3 \Rightarrow \overrightarrow{OG} : \overrightarrow{GP_2} = 1 : 2$
3. $\overrightarrow{P_1G} : \overrightarrow{P_1A} = 1 : 3 \Rightarrow \overrightarrow{P_1G} : \overrightarrow{GA} = 1 : 2$
4. Triangles OGP_1 and P_2GA are similar
5. Angles $\angle OP_1G$ and $\angle GAP_2$ are equal
6. Lines $OP_1 = l_3$ and $AP_2 = h_a$ are parallel
7. $h_a \perp a \Rightarrow l_3 \perp a$
8. l_3 is perpendicular bisector of BC
9. $P_1 = M_a$
10. $\overrightarrow{AG} : \overrightarrow{AM_a} = 2 : 3 \Rightarrow G$ is centroid of $\triangle ABC$

Automated generation of readable correctness proofs

- How can correctness proofs like the ones we have seen be automatically obtained?
- We need to formulate the problem statement and the set of lemmas, given as axioms and to pass them to some automated theorem prover

Problem statement

- ArgoTriCS can automatically generate the theorem (in a form suitable for ATPs) stating that the generated construction is correct

$$
\begin{aligned}
&\mathrm{inc}(A, l_1) \wedge \mathrm{inc}(H'_a, l_1) \wedge \\
&\mathrm{perp}(l_2, l_1) \wedge \mathrm{inc}(H'_a, l_2) \wedge \\
&\mathrm{circle}(O', A, c) \wedge \\
&\mathrm{inc}(B, l_2) \wedge \mathrm{inc}(C, l_2) \wedge \mathrm{inc\_c}(B, c) \wedge \mathrm{inc\_c}(C, c) \wedge B \neq C \implies \\
&H'_a = H_a \wedge O' = O
\end{aligned}
$$

- H'_a and O' are the points given, while H_a and O are the real altitude foot and circumcenter of constructed triangle ABC
- Various non-degeneracy conditions are added to the problem statement (e.g., $H'_a \neq A$, $A \neq B$, $A \neq C$, etc.) before it is given to ATPs

The axiom set for proof phase

- Definitions and lemmas identified by ArgoTriCS

$$\begin{aligned} \mathrm{inc}(A, h_a) &\wedge \mathrm{perp}(h_a, bc) \\ \overrightarrow{AG} : \overrightarrow{AM_a} &= 2 : 3 \end{aligned}$$

- Uniqueness lemmas

$$\begin{aligned} (\forall l)(\mathrm{inc}(A, l) \wedge \mathrm{perp}(l, bc) &\implies l = h_a) \\ (\forall c)(\mathrm{inc\_c}(A, c) \wedge \mathrm{inc\_c}(B, c) \wedge \mathrm{inc\_c}(C, c) &\implies c = c^\circ) \end{aligned}$$

- Properties of basic geometry predicates

$$\begin{aligned} (\forall l_1, l_2)(\mathrm{perp}(l_1, l_2) &\implies \mathrm{perp}(l_2, l_1)) \\ (\forall P_1, P_2)(\exists l)(\mathrm{inc}(P_1, l) &\wedge \mathrm{inc}(P_2, l)) \\ (\forall l1, l2, a)\ (\mathrm{perp}(l_1, a) \wedge \mathrm{para}(l_1, l_2) &\implies \mathrm{perp}(l_2, a)) \end{aligned}$$

Using automated theorem provers

- Problem statement and identified lemmas are formulated in TPTP format
- The conjecture is passed to automated theorem prover Vampire and coherent logic prover Larus
- Vampire is much more efficient, but Larus exports both readable proofs and formal proofs

Example of readable correctness proof

Axioms:

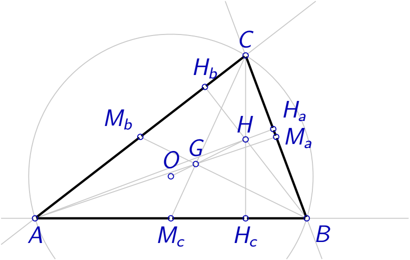
1. bc_unique : $\forall L\ (inc(pB, L) \wedge inc(pC, L) \Rightarrow L = bc\ )$
2. haA : $\forall H\ (perp(H, bc) \wedge inc(pA, H) \Rightarrow ha = H\ )$
3. pHa_def : $\forall H1\ (inc(H1, ha) \wedge inc(H1, bc) \Rightarrow H1 = pHa\ )$
4. cc_unique : $\forall C\ (inc\_c(pA, C) \wedge inc\_c(pB, C) \wedge inc\_c(pC, C) \Rightarrow C = cc\ )$
5. center_unique : $\forall C\ \forall C1\ \forall C2\ (center(C1, C) \wedge center(C2, C) \Rightarrow C1 = C2\ )$

Theorem: th_A_Ha_O0 :
$inc(pA, ha1) \wedge inc(pHa1, ha1) \wedge perp(ha1, a1) \wedge inc(pHa1, a1) \wedge inc\_c(pA, cc1) \wedge center(pOc1, cc1) \wedge inc\_c(pB, cc1) \wedge inc(pB, a1) \wedge inc\_c(pC, cc1) \wedge inc(pC, a1) \Rightarrow pHa = pHa1$
Proof:

1. $pHa = pHa$ (by MP, using axiom eqnativeEqSub0; instantiation: $A \mapsto pHa$, $B \mapsto pHa$, $X \mapsto pHa$)
2. $a1 = bc$ (by MP, from $inc(pB, a1)$, $inc(pC, a1)$ using axiom bc_unique; instantiation: $L \mapsto a1$)
3. $perp(ha1, bc)$ (by MP, from $perp(ha1, a1)$, $a1 = bc$ using axiom perpEqSub1; instantiation: $A \mapsto ha1$, $B \mapsto a1$, $X \mapsto bc$)
4. $ha = ha1$ (by MP, from $perp(ha1, bc)$, $inc(pA, ha1)$ using axiom haA; instantiation: $H \mapsto ha1$)
5. $inc(pHa1, ha)$ (by MP, from $inc(pHa1, ha1)$, $ha = ha1$ using axiom incEqSub1; instantiation: $A \mapsto pHa1$, $B \mapsto ha1$, $X \mapsto ha$)
6. $inc(pHa1, bc)$ (by MP, from $inc(pHa1, a1)$, $a1 = bc$ using axiom incEqSub1; instantiation: $A \mapsto pHa1$, $B \mapsto a1$, $X \mapsto bc$)
7. $pHa1 = pHa$ (by MP, from $inc(pHa1, ha)$, $inc(pHa1, bc)$ using axiom pHa_def; instantiation: $H1 \mapsto pHa1$)
8. $pHa = pHa1$ (by MP, from $pHa1 = pHa$, $pHa = pHa$ using axiom eqnativeEqSub0; instantiation: $A \mapsto pHa$, $B \mapsto pHa1$, $X \mapsto pHa$)
9. Proved by assumption! (by QEDas)

Results

- The subset of problems from Wernick's corpus is considered: 35 non-isomorphic solvable location triangle problems over
  - vertices A, B, C
  - side midpoints M_a, M_b, M_c
  - feet of altitudes H_a, H_b, H_c
  - centroid G, circumcenter O and orthocenter H



- Vampire succesfully proved 31 problem
- Larus successfully proved 20 problems within the given time-limit of 300 seconds

Conclusions

- Work-in-progress
- First step toward automated readable, synthetic, formally verified correctness proofs
- Important for educational purposes
- Lemmas identified during development of ArgoTriCS were needed, but they were not sufficient
- Coherent logic provers are still not as efficient as automated theorem provers

Future work

- Proofs currently rely on high-level lemmas
- Correctness of used lemmas should be proved: we are currently developing formal Isabelle/HOL proofs for all lemmas from the basic geometric axioms
- We plan to consider degenerate cases and existence of constructed objects
- We plan to exploit concept of hints avaliable in Larus, to help it prove some more conjectures