Geometrisation of Geometry

Predrag Janičić

Faculty of Mathematics
University of Belgrade, Serbia

ADG 2016, Strasbourg, France, June 27-29, 2016.

Automated Theorem Proving in Geometry

- Many successes over the previous sixty years:
  - algebraic provers (Wu's method, GB method)
  - semi-synthetic provers (area method, full angle method,...)
- But there are still many challenges, some of which are:
  - proving for $\forall\exists$ fragment
  - generating synthetic proofs
  - generating human-readable proofs
- For the above – coherent logic (CL) can help, to some extent

Coherent Logic in Geometry

- Using CL in geometry was one of subjects of my work over the previous >20 years
- Together with:
  - Marc Bezem
  - Stevan Kordić
  - Vesna Marinković (Pavlović)
  - Julien Narboux
  - Mladen Nikolić
  - Pascal Schreck
  - Sana Stojanović Đurđević

What is Coherent Logic?

- A FOL formula is said to be *coherent* if is of the form:

$$A_1(\vec{x}) \wedge \ldots \wedge A_n(\vec{x}) \Rightarrow \exists \vec{y}(B_1(\vec{x},\vec{y}) \vee \ldots \vee\ B_m(\vec{x},\vec{y}))$$

  where universal closure is assumed, $0 \leq n$, $0 \leq m$, A_i denote atomic formulae, B_i denote conjunctions of atomic formulae
- CL formulae are sometimes called *geometric*, but more often it is assumed that *geometric formulae* allow *infinitary disjunctions*
- A number of authors, in different contexts point to this fragment of FOL, as suitable for automation, readability etc.

Properties of Coherent Logic

- CL is simple, allows simple forward chaining proofs
- Human-readable, natural language proofs can be easily obtained
- Machine verifiable proofs (for proof assistants) can be easily obtained

Coherent Logic – Toy Example

- Axioms:
  - $p(x) \Rightarrow \exists y(r(x,y) \vee q(x,y))$
  - $r(x,y) \Rightarrow s(x,y)$
  - $q(x,y) \Rightarrow s(x,y)$
- Theorem: $p(x) \Rightarrow \exists y\ s(x,y)$
- Proof sketch:
  - $p(a)$, for new a
  - $p(a)$ implies there is b such that $r(a,b) \vee q(a,b)$
  - if $r(a,b)$ then $s(a,b)$
  - if $q(a,b)$ then $s(a,b)$
  - QED

Coherentisation/Geometrisation

- Coherentisation/Geometrisation: Any first-order theory can be translated into CL (possibly with additional predicate symbols)
- One FOL formula may give several CL formulae
- In translations, negations are pushed down to atomic formulae and for every predicate symbol R, a new symbol $\overline{R}$ stands for $\neg R$, with $\forall \vec{x}(R(\vec{x}) \wedge \overline{R}(\vec{x}) \Rightarrow \bot)$, $\forall \vec{x}(R(\vec{x}) \vee \overline{R}(\vec{x}))$
- If a CL formula can be classically proved from a set of CL formulae, then it can be also constructively proved
- Translation from FOL to CL is not necessarily constructive

Provability and Proof System

- The problem of provability in coherent logic is semi-decidable
- CL admits a simple proof system, such as:

$$\frac{\Gamma, ax, A_1(\vec{a}), \ldots, A_n(\vec{a}), \underline{B_1(\vec{a},\vec{b}) \vee \ldots \vee B_m(\vec{a},\vec{b})} \vdash P}{\Gamma, ax, A_1(\vec{a}), \ldots, A_n(\vec{a}) \vdash P} \; emp \; (extended \; mp)$$

where $ax = A_1(\vec{x}) \wedge \ldots \wedge A_n(\vec{x}) \Rightarrow \exists \vec{y}(B_1(\vec{x},\vec{y}) \vee \ldots \vee B_m(\vec{x},\vec{y}))$

$$\frac{\Gamma, \underline{B_1(\vec{c})} \vdash P \quad \ldots \quad \Gamma, \underline{B_n(\vec{c})} \vdash P}{\Gamma, B_1(\vec{c}) \vee \ldots \vee B_m(\vec{c}) \vdash P} \; cs \; (case \; split)$$

$$\frac{}{\Gamma, \underline{B_i(\vec{a},\vec{b})} \vdash \exists \vec{y}(B_1(\vec{a},\vec{y}) \vee \ldots \vee B_m(\vec{a},\vec{y}))} \; as \; (assumption)$$

$$\frac{}{\Gamma, \bot \vdash P} \; efq \; (ex \; falso \; quodlibet)$$

- Any CL proof can be represented as

$$proof \; ::= \; emp^* \left(cs \left(proof^{\geq 2} \right) \mid as \mid efq \right)$$

Proof System – Toy Example

- AX:
  - $p(x) \Rightarrow \exists y(r(x,y) \vee q(x,y))$
  - $r(x,y) \Rightarrow s(x,y)$
  - $q(x,y) \Rightarrow s(x,y)$
- Theorem: $p(x) \Rightarrow \exists y\ s(x,y)$

$$\dfrac{\dfrac{\dfrac{\overline{AX, p(a), r(a,b), s(a,b) \vdash \exists y\ s(a,y)}}{AX, p(a), r(a,b) \vdash \exists y\ s(a,y)} \qquad \dfrac{\overline{AX, p(a), q(a,b), s(a,b) \vdash \exists y\ s(a,y)}}{AX, p(a), q(a,b) \vdash \exists y\ s(a,y)}}{AX, p(a), \underline{r(a,b) \vee q(a,b)} \vdash \exists y\ s(a,y)}}{AX, p(a) \vdash \exists y\ s(a,y)}$$

Automated provers for CL

- Euclid (Janičić and Kordić, 1992), Prolog, specialized for Euclidean geometry; export to natural language
- ArgoCLP (Stojanović, Pavlović, Janičić, 2010), C++, export to natural language and Isabelle, automated simplification of proofs
- CL (Bezem), export to Coq; used for proving Hessenberg's theorem: Pappus' axiom implies Desargues' axiom
- GeologUI (Fisher), with graphical interface
- coherent (Berghofer), ML, within Isabelle
- Geo (De Nivelle), with learning lemmas
- Calypso (Nikolić and Janičić), based on CDCL SAT solving

Theorem: Assuming that $\alpha \neq \beta$, the line p is incident to the plane α, the line p is incident to the plane β, the point A is incident to the plane α, and the point A is incident to the plane β, show that the point A is incident to the line p.

Proof:

Let us prove that the point A is incident to the line p by reductio ad absurdum.

1. Assume that the point A is not incident to the line p.
    2. There exist a point B and a point C such that the point B is incident to the line p, $B \neq C$ and the point C is incident to the line p (by axiom ax_I3a).
    3. From the facts that the line p is incident to the plane α, and the point B is incident to the line p, it holds that the point B is incident to the plane α (by axiom ax_D11).
    4. From the facts that the line p is incident to the plane β, and the point B is incident to the line p, it holds that the point B is incident to the plane β (by axiom ax_D11).
    5. From the facts that $B \neq C$, the point B is incident to the line p, the point C is incident to the line p, and the point A is not incident to the line p, it holds that the points B, C and A are not collinear (by axiom ax_D1a).
    6. From the facts that the line p is incident to the plane α, and the point C is incident to the line p, it holds that the point C is incident to the plane α (by axiom ax_D11).
    7. From the facts that the line p is incident to the plane β, and the point C is incident to the line p, it holds that the point C is incident to the plane β (by axiom ax_D11).
    8. From the facts that the points B, C and A are not collinear, it holds that the points A, B and C are not collinear (by axiom ax_ncol_231).
    9. From the facts that the points A, B and C are not collinear, the point A is incident to the plane α, the point B is incident to the plane α, the point C is incident to the plane α, the point A is incident to the plane β, the point B is incident to the plane β, and the point C is incident to the plane β, it holds that $\alpha = \beta$ (by axiom ax_I5).
    10. From the facts that $\alpha = \beta$, and $\alpha \neq \beta$ we get a contradiction.

        Contradiction.

Therefore, it holds that the point A is incident to the line p.

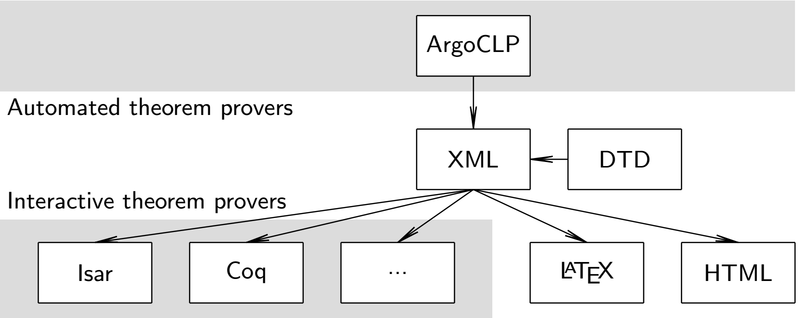
This proves the conjecture.

CL Vernacular

- *Vernacular* is the everyday, ordinary language of the people of some region
- De Bruijn used the syntagm, trying to "put a substantial part of the mathematical vernacular into the formal system"
- Wiedijk: "Apparently there is a canonical style of presenting mathematics that people discover independently: something like a *natural* mathematical vernacular."
- The language discussed by Wiedijk is closely related to the CL proof language

CL Vernacular support

- A proof representation called "coherent logic vernacular" can link different proof formats and tools
- The proposed proof representation is accompanied by a corresponding XML format, specified by a DTD



```
Theorem th_4_19 : ∀ (A:point) (B:point) (C:point) (D:point), (bet A B C ∧ cong A B A D ∧ cong C
B C D) → B = D.
Proof.
 intros.
 assert (bet B A A) by applying (th_3_1 B A ) .
 assert (col C A B) by applying (ax_4_10_3 A B C ) .
 assert (cong A D A B) by applying (th_2_2 A B A D ) .
 assert (A = B ∨ A ≠ B) by applying (ax_g1 A B ) .
 by cases on (A = B ∨ A ≠ B).
 - {
   assert (cong A D A A) by (substitution).
   assert (A = D) by applying (ax_3 A D A ) .
   assert (B = D) by (substitution).
   conclude.
   }
 - {
   assert (A = C ∨ A ≠ C) by applying (ax_g1 A C ) .
   by cases on (A = C ∨ A ≠ C).
   - {
     assert (bet A B A) by (substitution).
     assert (A = B) by applying (th_3_4 A B A ) .
     assert (False) by (substitution).
     contradict.
     }
   - {
     assert (C ≠ A) by (substitution).
     assert (B = D) by applying (th_4_18 C A B D ) .
     conclude.
     }
   }
Qed.
```

CL-based Formalizations of Geometry

- Large portions of geometry can be easily transformed into CL
- Case study: *Metamathematische Methoden in der Geometrie*, by Wolfram Schwabhäuser, Wanda Szmielew, and Alfred Tarski
- This book has been a subject of several automation and formalization projects
- Geometry in this book is expressed in terms of FOL with equality, with *points* as the only primitive objects and with two primitive predicate symbols – *cong* and *bet* (for betweeness)
- There are only eleven axioms

Schwabhäuser-Szmielew-Tarski axioms

Axiom A1: $cong(A, B, B, A)$

Axiom A2: $cong(A, B, P, Q) \wedge cong(A, B, R, S) \Rightarrow cong(P, Q, R, S)$

Axiom A3: $cong(A, B, C, C) \Rightarrow A = B$

Axiom A4: $\exists X\ (bet(Q, A, X) \wedge cong(A, X, B, C))$

Axiom A5: $A \neq B \wedge bet(A, B, C) \wedge bet(A', B', C') \wedge cong(A, B, A', B') \wedge cong(B, C, B', C') \wedge cong(A, D, A', D') \wedge cong(B, D, B', D') \Rightarrow cong(C, D, C', D')$

Axiom A6: $bet(A, B, A) \Rightarrow A = B$

Axiom A7: $bet(A, P, C) \wedge bet(B, Q, C) \Rightarrow \exists X\ (bet(P, X, B) \wedge bet(Q, X, A))$

Axiom A8: $\exists A\ \exists B\ \exists C\ (\neg bet(A, B, C) \wedge \neg bet(B, C, A) \wedge \neg bet(C, A, B))$

Axiom A9: $P \neq Q \wedge cong(A, P, A, Q) \wedge cong(B, P, B, Q) \wedge cong(C, P, C, Q) \Rightarrow (bet(A, B, C) \vee bet(B, C, A) \vee bet(C, A, B))$

Axiom A10: $bet(A, D, T) \wedge bet(B, D, C) \wedge A \neq D \Rightarrow \exists X\ \exists Y\ (bet(A, B, X) \wedge bet(A, C, Y) \wedge bet(X, T, Y))$

Axiom A11: $\forall \Phi\ \forall \Psi\ \exists A\ \forall X\ \forall Y\ ((X \in \Phi \wedge Y \in \Psi \Rightarrow bet(A, X, Y)) \Rightarrow \exists B\ \forall X\ \forall Y\ (X \in \Phi \wedge Y \in \Psi \Rightarrow bet(X, B, Y))$

Coherentisation and Proving Method

- The process of coherentisation of the axioms and theorems was straightforward
- From the original 179 theorems (from chapters 1 to 12 of the book), the process gave 238 CL formulae (while 5 schematic theorems involving n-tuples were considered only for $n = 2$)
- The proving process for one theorem goes as follows:
  - All axioms and theorems that precede the theorem are passed to resolution provers (Vampire, E, and SPASS)
  - If one of the resolution provers proves the conjecture, the list of used axioms/theorems is used for proving the conjecture again until the list of used axioms/theorems remains unchanged
  - With the obtained list of axioms/theorems, ArgoCLP prover is invoked, and (if successful) the proof is exported in the CL vernacular XML format

Results and Outputs

- ArgoCLP (supported by resolution provers) proved 37% of the theorems automatically
- One of the outputs of the study: a digital version of the book, with all axioms, definitions, theorems, and generated proofs filled-in, all in the natural language form

Results and Outputs – Example

Chapter 3

Simple Properties of Betweenness

Theorem 9 (th_3_1.) *It holds that* $bet(A, B, B)$.

Proof:
1. There exist a point G where $bet(A, B, G)$ and $BG \cong AA$ (using ax_4).
2. From the facts $BG \cong AA$ it holds that $B = G$ (using ax_3).
3. From the facts $bet(A, B, G)$ and $B = G$ it holds that $bet(A, B, B)$.
4. From the facts $bet(A, B, B)$ we proved a conjecture.

QED

Theorem 10 (th_3_2.) *Assuming that* $bet(A, B, C)$ *it holds that* $bet(C, B, A)$.

Proof:
1. It holds that $bet(A, B, B)$ (using th_3_1).
2. It holds that $bet(B, B, B)$ (using th_3_1).
3. It holds that $bet(B, C, C)$ (using th_3_1).
4. From the facts $bet(A, B, B)$ and $bet(B, B, B)$ there exist a point F where $bet(B, F, B)$ and $bet(B, F, A)$ (using ax_7).
5. From the facts $bet(B, F, B)$ it holds that $B = F$ (using ax_6).
6. From the facts $bet(A, B, C)$ and $bet(B, C, C)$ there exist a point I where $bet(B, I, B)$ and $bet(C, I, A)$ (using ax_7).
7. From the facts $bet(B, I, B)$ it holds that $B = I$ (using ax_6).
8. From the facts $bet(C, I, A)$ and $B = F$ and $B = I$ it holds that $bet(C, B, A)$.
9. From the facts $bet(C, B, A)$ we proved a conjecture.

QED

Theorem 11 (th_3_3.) *It holds that* $bet(A, A, B)$.

Proof:

17

CL and Construction Problems

- Statements of the form $\forall\exists$ naturally arise in geometry, for instance – in construction problems
- For a construction problem, roughly said, the task is to *prove constructively* a theorem of the form:

$$\forall\vec{x}\exists\vec{y}\ \Psi(\vec{x};\vec{y})$$

- Sometimes even more (solution exists iff $\Phi(\vec{x})$):

$$\forall\vec{x}(\Phi(\vec{x}) \Rightarrow \exists\vec{y}\ \Psi(\vec{x};\vec{y})\ \wedge\ \neg\Phi(\vec{x}) \Rightarrow \neg\exists\vec{y}\ \Psi(\vec{x};\vec{y}))$$

CL and Construction Problems – Example

- Example (Wernick's problem 4): *Given points A, B, and G, construct a triangle ABC, such that G is the centroid of ABC.*
- A careful analysis leads to the theorem that gives a full characterization of solvability:

$$\forall A, B, G\ (\neg collinear(A, B, G) \Leftrightarrow$$

$$\exists C.(\neg collinear(A, B, C) \wedge centroid(G, A, B, C)))$$

- With the help of our solver for construction problems ArgoTriCS, the above conjectures can be proved by ArgoCLP

Compendium of Construction Problems

The list of Wernick's problems

Statuses of all problems: *S (s)* denotes that the problem is solvable and its solution is given, *S (ns)* denotes that the problem is proved solvable but its solution is not given, *L* that the problem is locus dependent, *R* that the problem is redundant, while *U* denotes that the problem is unsolvable.

1. A, B, C *S (s)*	2. A, B, O *L*	3. A, B, M_a *S (s)*	4. A, B, M_b *S (s)*	5. A, B, M_c *R*
6. A, B, G *S (s)*	7. A, B, H_a *L*	8. A, B, H_b *L*	9. A, B, H_c *L*	10. A, B, H *S (s)*
11. A, B, T_a *S (s)*	12. A, B, T_b *S (s)*	13. A, B, T_c *L*	14. A, B, I *S (s)*	15. A, C, O *L*
16. A, C, M_a *S (s)*	17. A, C, M_b *R*	18. A, C, M_c *S (s)*	19. A, C, G *S (s)*	20. A, C, H_a *L*
21. A, C, H_b *L*	22. A, C, H_c *L*	23. A, C, H *S (s)*	24. A, C, T_a *S (s)*	25. A, C, T_b *L*
26. A, C, T_c *S (s)*	27. A, C, I *S (s)*	28. A, O, M_a *S (s)*	29. A, O, M_b *L*	30. A, O, M_c *L*
31. A, O, G *S (s)*	32. A, O, H_a *S (s)*	33. A, O, H_b *S (s)*	34. A, O, H_c *S (s)*	35. A, O, H *S (s)*
36. A, O, T_a *S (s)*	37. A, O, T_b *S (s)*	38. A, O, T_c *S (s)*	39. A, O, I *S (s)*	40. A, M_a, M_b *S (s)*
41. A, M_a, M_c *S (s)*	42. A, M_a, G *R*	43. A, M_a, H_a *L*	44. A, M_a, H_b *S (s)*	45. A, M_a, H_c *S (s)*
46. A, M_a, H *S (s)*	47. A, M_a, T_a *S (s)*	48. A, M_a, T_b *U*	49. A, M_a, T_c *U*	50. A, M_a, I *S (s)*
51. A, M_b, M_c *S (s)*	52. A, M_b, G *S (s)*	53. A, M_b, H_a *L*	54. A, M_b, H_b *L*	55. A, M_b, H_c *L*
56. A, M_b, H *S (s)*	57. A, M_b, T_a *S (s)*	58. A, M_b, T_b *L*	59. A, M_b, T_c *S (s)*	60. A, M_b, I *S (s)*
61. A, M_c, G *S (s)*	62. A, M_c, H_a *L*	63. A, M_c, H_b *L*	64. A, M_c, H_c *L*	65. A, M_c, H *S (s)*
66. A, M_c, T_a *S (s)*	67. A, M_c, T_b *S (s)*	68. A, M_c, T_c *L*	69. A, M_c, I *S (s)*	70. A, G, H_a *L*
71. A, G, H_b *S (s)*	72. A, G, H_c *S (s)*	73. A, G, H *S (s)*	74. A, G, T_a *S (s)*	75. A, G, T_b *U*
76. A, G, T_c *U*	77. A, G, I *S (s)*	78. A, H_a, H_b *S (s)*	79. A, H_a, H_c *S (s)*	80. A, H_a, H *L*
81. A, H_a, T_a *L*	82. A, H_a, T_b *S (s)*	83. A, H_a, T_c *S (s)*	84. A, H_a, I *S (s)*	85. A, H_b, H_c *S (s)*
86. A, H_b, H *L*	87. A, H_b, T_a *S (s)*	88. A, H_b, T_b *L*	89. A, H_b, T_c *S (s)*	90. A, H_b, I *S (s)*
91. A, H_c, H *L*	92. A, H_c, T_a *S (s)*	93. A, H_c, T_b *S (s)*	94. A, H_c, T_c *L*	95. A, H_c, I *S (s)*
96. A, H, T_a *S (s)*	97. A, H, T_b *U*	98. A, H, T_c *U*	99. A, H, I *S (ns)*	100. A, T_a, T_b *S (s)*
101. A, T_a, T_c *S (s)*	102. A, T_a, I *L*	103. A, T_b, T_c *S (s)*	104. A, T_b, I *S (s)*	105. A, T_c, I *S (s)*
106. B, C, O *L*	107. B, C, M_a *R*	108. B, C, M_b *S (s)*	109. B, C, M_c *S (s)*	110. B, C, G *S (s)*
111. B, C, H_a *L*	112. B, C, H_b *L*	113. B, C, H_c *L*	114. B, C, H *S (s)*	115. B, C, T_a *L*
116. B, C, T_b *S (s)*	117. B, C, T_c *S (s)*	118. B, C, I *S (s)*	119. B, O, M_a *L*	120. B, O, M_b *S (s)*
121. B, O, M_c *L*	122. B, O, G *S (s)*	123. B, O, H_a *S (s)*	124. B, O, H_b *S (s)*	125. B, O, H_c *S (s)*
126. B, O, H *S (s)*	127. B, O, T_a *S (s)*	128. B, O, T_b *S (s)*	129. B, O, T_c *S (s)*	130. B, O, I *S (s)*

CL and Geometry Illustrations

- In geometry and in the whole of mathematics, illustrations are often very valuable, but almost always just an informal content
- Links between proofs and illustration are loose: proofs do not rely on illustrations, illustrations are not derived from proofs
- However, CL proofs, in some cases, can be used for automated generation of illustrations
- The idea is not to instruct a CL prover to generate illustrations, but to generate illustrations from CL proofs
- Hence, *proofs can carry information for illustrations*

CL and Geometry Illustrations (2)

- In CL proofs, axioms of the following form are used:
  $A_1(\vec{x}) \wedge \ldots \wedge A_n(\vec{x}) \Rightarrow \exists \vec{y}(B_1(\vec{x}, \vec{y}) \vee \ldots \vee\ B_m(\vec{x}, \vec{y}))$
- Each axiom with $m > 0$ (i.e., introducing news objects) need to have an *associated illustration rule*
- For example, an axiom *for any two points A and B, there is a point C such that bet*(A, B, C) can be modeled in GCLC in the following way:

```
random r
expression r' {1+r}
towards C A B r'
```

CL and Geometry Illustrations (3)

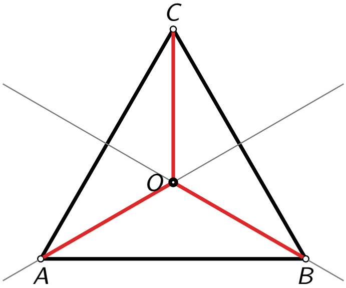
- If the conjecture being proved has the form: $\forall \vec{x}(\Phi(\vec{x}) \Rightarrow \exists \vec{y}\ \Psi(\vec{x}; \vec{y}))$ in order to illustrate it, one must have initial objects $\vec{x}$ meeting conditions $\Phi(\vec{x})$
- So, the first step is to prove that $\Phi(\vec{x})$ is consistent (if it is not, the statement is trivially valid), i.e., to prove $\exists \vec{x}\ \Phi(\vec{x})$
- A constructive proof of this conjecture will give one model for $\Phi(\vec{x})$ and will serve as a basis for an illustration for the main proof
- This step may not be easy and it actually involves solving a geometry construction problem

CL and Geometry Illustrations – Example

Artificial example:

- *Given the points* A*,* B*,* C*, such that* $A \neq B$*,* $AB \cong AC$*, and* $AB \cong BC$*, prove there is a point* O *such that* $OA \cong OB \cong OC$
- First step: prove *there are points* A*,* B*,* C*, such that* $A \neq B$*,* $AB \cong AC$*, and* $AB \cong BC$
- This gives one (say, Cartesian) model
- Second step: interpret each step of the main proof as illustration step (using the illustration rules)

CL and Geometry Illustrations – Example (2)



Conclusions and Possible Directions for Future Work

- Coherent logic can have applications in automated deduction in geometry:
  - in producing human-readable proofs,
  - in producing machine verifiable proofs,
  - in proving statements of the form $\forall\exists$,
  - in producing illustrations automatically from proofs
- CL provers not very powerful on their own, but powerful in synergy with other tools
- It would be interesting to construct suitable sets of CL geometry lemmas that can be used in proving higher-level conjectures