CASC'2013 - Berlin (9th-13th September)

A Note on the Need for Radical Membership Checking in Mechanical Theorem Proving in Geometry

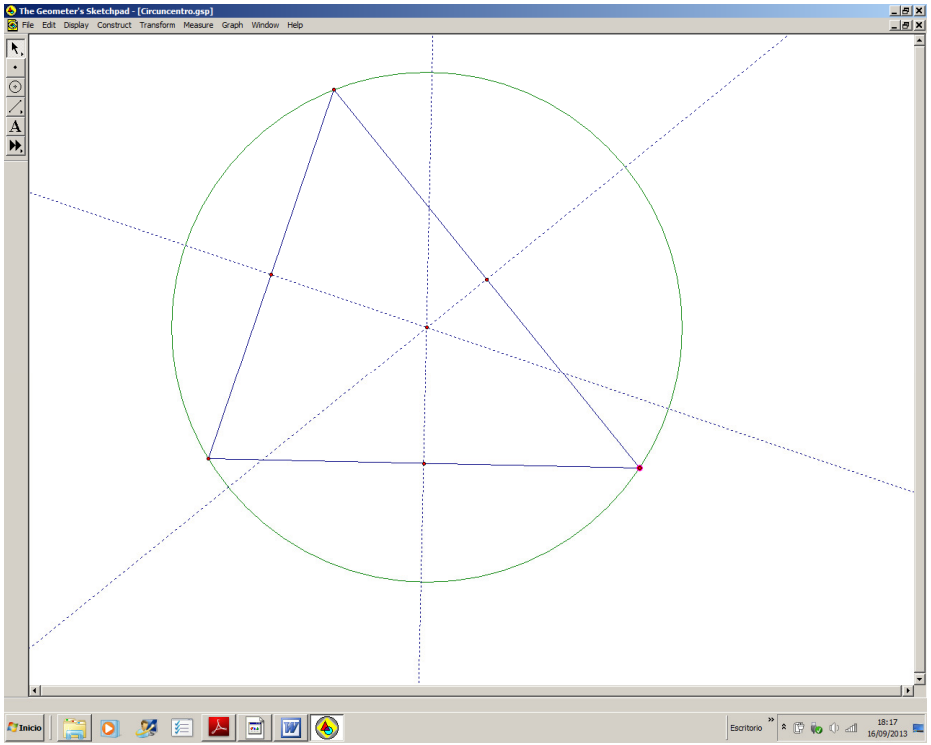
Eugenio Roanes-Lozano & Eugenio Roanes-Macías

Algebra Dept., Universidad Complutense de Madrid (Spain)

{eroanes,roanes}@mat.ucm.es

1 INTRODUCTION

1.1 Existence of circumcentre with the DGS *GSP 4*



(or with any other usual DGS –that performs numeric computations). Observe that this IS NOT proving, but checking.

We are thinking about PROVING in the mathematical sense.

1.2 Synthetic proof of the existence of circumcentre

Let: $D = m_{AB} \cap m_{BC}$

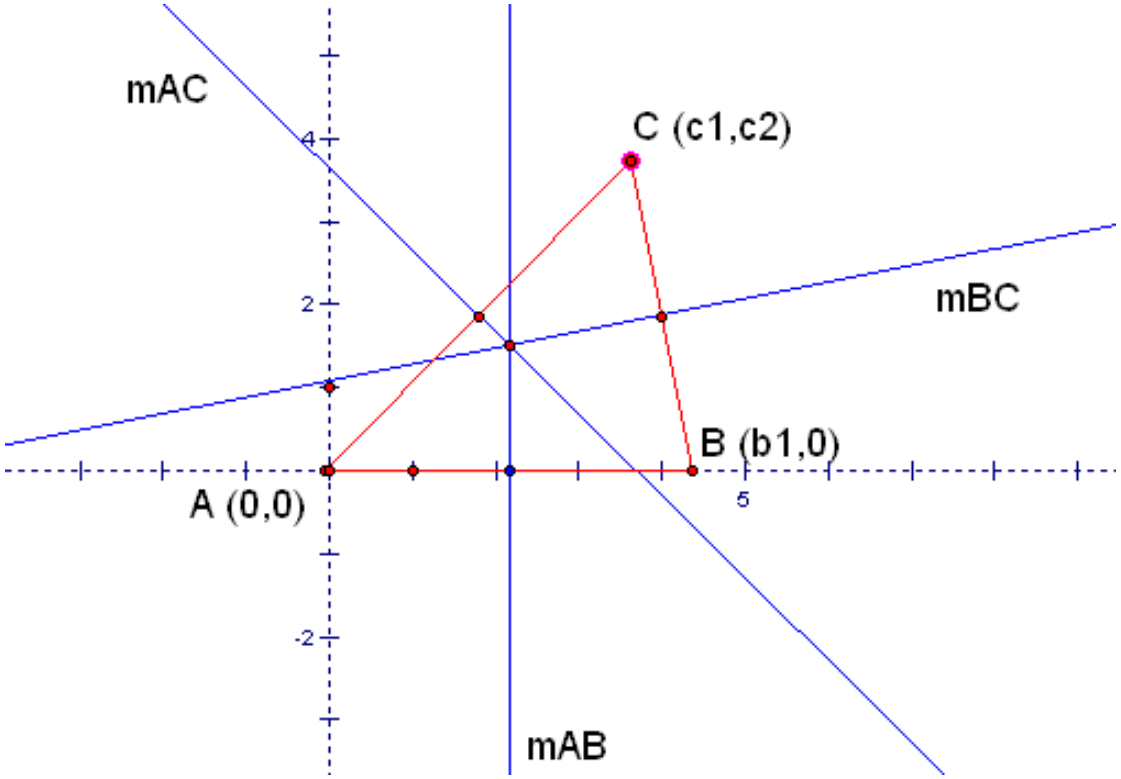
then: $dist(D,A) = dist(D,B)$
and: $dist(D,B) = dist(D,C)$

consequently: $dist(D,A) = dist(D,C)$

and therefore: $D \in m_{AC}$

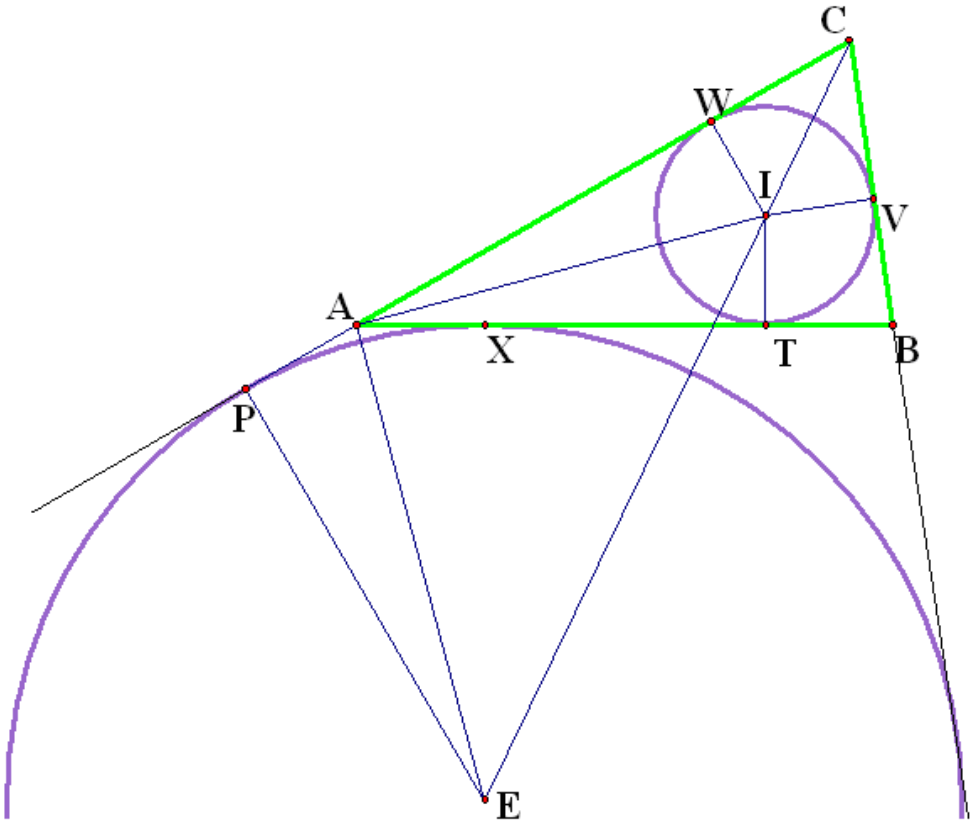
so all three perpendicular bisectors are concurrent.

1.3 Algebraic (mech.) proof of the existence of circumcentre



The system of linear equations involving the equations of the three perpendicular bisectors is compatible (and has a single unique solution).

1.4 Algebraic (mech.) proof: a not so simple example



Linear system solving (Gauss method) is not enough.

Algebraic polynomial systems arise (Gröbner bases).

2 SOME NOTES ABOUT ALGEBRAIC GEOMETRY

Definition1: An ideal of a ring is a special subset of a ring such that it is also a ring and the product of any element of the ring by an element of the subset is again in the subset. Ex.: *3Z* is an ideal of *Z*.

Definition 2: The radical of an ideal *I*, *Rad(I)*, is the set of elements, α, such that some integer power of α is in *I*. Ex.: *Rad(9Z) = 3Z*.

Proposition 1: *Rad(I)* is also an ideal and, obviously, $I \subseteq Rad(I)$.

Definition 3: A basis of an ideal is a set of generators of the ideal (i.e., the elements of the ideal are the linear algebraic combinations of the elements in the basis). The ideal generated by the polynomials $p_1,...,p_n$ is denoted $<p_1,...,p_n>$.

Corollary 1: $<1>$ is the whole ring.

Property 1: A Groebner basis of a polynomial ideal is a very special basis.

Once the way the monomials have to be ordered and the order for the variables are fixed, the (reduced) Groebner basis (GB) of an ideal is unique.

Buchberger's algorithm provides a method to obtain the GB of any ideal of a polynomial ring over a field in a finite number of variables.

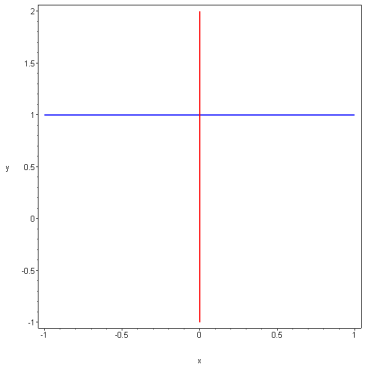
Corollary 2: Checking some very complex algebraic issues turns easily decidable. For instance, checking whether two ideals of a polynomial ring are equal or not can be decided by simply comparing their GB.

Definition 4: An algebraic variety is the set of solutions of a system of polynomial equations (i.e., the set of zeros of the ideal generated by the corresponding polynomials).
v(I) denotes the algebraic variety of ideal *I*.

Definition 5: The ideal of an algebraic variety *V*, *i(V)*, is the set of all polynomials which vanish on all the points of the set *V*.
i(V) turns out to be an ideal.

Theorem 1: Hilbert's Nullstellensatz states that, if the base field is algebraically closed, then: *i(v(I))=Rad(I)*.

Example: (base field ***C***)



$v(\langle x^3, y-1\rangle) = \{(0,1)\}$

$i(v(\langle x^3, y-1\rangle)) = \langle x, y-1\rangle = Rad(\langle x^3, y-1\rangle)$

Proposition 2: (radical membership criterion) Let $K[x_1,...,x_n]$ be a polynomial ring over the field K, let $p \in K[x_1,...,x_n]$ and let $I=\langle p_1,...,p_m\rangle$ be an ideal of $K[x_1,...,x_n]$. Let w be another variable, independent from $x_1,...,x_n$. Then:

$p \in Rad(I)$ (in the polynomial ring $K[x_1,...,x_n]$) $\Leftrightarrow$

$\Leftrightarrow$ the ideal $\langle p_1,...,p_m,1-p\cdot w\rangle$ of $K[x_1,...,x_n,w]$ is the whole ring, $\langle 1\rangle$.

3 MECHANICAL TH. PROVING IN GEOMETRY

3.1 Idea of Chou's approach

Let *H* be the ideal describing the hypotheses polynomials and let *t* be the thesis polynomial.

1st Step (ideal membership –sufficient condition):

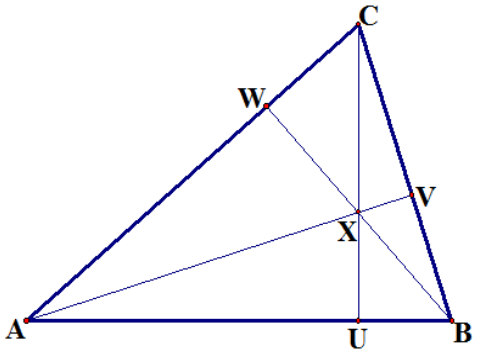
If $t \in H$, then *t* is a linear algebraic combination of some of the elements in *H*. Consequently, at the points where all the polynomials in *H* vanish, any linear algebraic combination of these polynomials will vanish, so *t* will also vanish. Consequently, $v(H)$ is a subset of $v(<t>)$. Therefore, according to the ideas above, the theorem is "generally true".

2nd Step (radical membership –necessary. and sufficient condition):

t belongs to $Rad(H)$ iff the theorem is "generally true".

- Example

ORTHOCENTER.MWS



Auxiliary procedures

Condition for points *M, N, P* to be collinear:

```
> colinea:=proc(M,N,P)
>   (N[1]-M[1])*(P[2]-M[2])-(N[2]-M[2])*(P[1]-M[1])
>   end:
```

Condition for line passing through points U, V and line passing through points W, Y to be *orthogonal:*

```
> ortog:=proc(U,V,W,Y)  #UV orthogonal WY
>   (Y[1]-W[1])*(V[1]-U[1])+(Y[2]-W[2])*(V[2]-U[2])
>   end:
```

Coordinates of points

Vertices of triangle ABC:

```
> A:=[0,0]:  B:=[b,0]:   C:=[c,e]:
```

Orthogonal projections of vertices on oposite line-sides of ABC:

```
> U:=[u,0]:  V:=[v1,v2]:  W:=[w1,w2]:
```

Intersection point, X, of two altitudes of ABC:

```
> X:=[x,y]:
```

Thesis condition and its corresponding thesis polynomial

Point X is in line CU:

```
> thesis:=colinea(C,X,U);
```

$$thesis := -(x - c)\, e - (y - e)\, (u - c)$$

Hypothesis conditions and their corresponding hypothesis polynomials

(about collinearity and orthogonality conditions)

H1) lines CU and AB are orthogonal:

```
> h1:=ortog(C,U,A,B);
```

$$h1 := b\, (u - c)$$

H2) points B, V, C are collinear:

```
> h2:=colinea(B,V,C);
```

$$h2 := (v1 - b)\, e - v2\, (c - b)$$

...

...

List of hypothesis polinomials:

```
> listHyp:=[h1, h2, h3, h4, h5, h6, h7]:
```

Thesis condition and its corresponding thesis polynomial

Point X is in line CU:

```
> thesis:=colinea(C,X,U);
```

$$thesis := -(x - c)\, e - (y - e)\, (u - c)$$

List of hypothesis and thesis polinomials:

```
> listHypThesis:=[h1, h2, h3, h4, h5, h6, h7, thesis];
```

Method of equal Groebner Bases

```
> with(Groebner):
> GB1:=Basis( listHyp, plex(var) );
```

$$GB1 := [-c\,b + y\,e + c^2,\ x - c,\ w2\,c^2 - c\,b\,e + e^2\,w2,\ c^2\,w1 - c^2\,b + e^2\,w1,$$
$$b^2\,v2 - b^2\,e + c\,b\,e - 2\,b\,v2\,c + v2\,c^2 + v2\,e^2,\ v1\,c^2 - 2\,c\,v1\,b + v1\,b^2 + e^2\,v1 - e^2\,b,$$
$$u - c]$$

```
> GB2:=Basis( listHypThesis, plex( var ) );
```

$$GB2 := [-c\,b + y\,e + c^2,\ x - c,\ w2\,c^2 - c\,b\,e + e^2\,w2,\ c^2\,w1 - c^2\,b + e^2\,w1,$$
$$b^2\,v2 - b^2\,e + c\,b\,e - 2\,b\,v2\,c + v2\,c^2 + v2\,e^2,\ v1\,c^2 - 2\,c\,v1\,b + v1\,b^2 + e^2\,v1 - e^2\,b,$$
$$u - c]$$

```
> evalb(GB1=GB2);
```

$$true$$

Method of Groebner Basis <1>

(Based on radical membership)

```
> Basis([h1, h2, h3, h4, h5, h6, h7, 1-z*thesis],plex( var,z ));
```

$$[1]$$

3.2 Chou's remark

- Shang-Ching Chou: *Mechanical Geometry Theorem Proving*. Reidel, 1988.

  http://books.google.es/books?id=R8iDSMbDC-kC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

- In page 78, we can find **Method (2.4)**, and, in it:

  "Step 1 can be considered as a first approximation. However, for all theorems we have found in practice, *J=L*. Thus, step 1 is usually sufficient."

4 PECH'S COUNTEREXAMPLE

- Pavel Pech: *On the need of radical ideals in automatic proving: a theorem about regular polygons*, in: Botana, F., Recio, T. (eds.) Proc. ADG 2006, pp. 157-170. Springer-Verlag, LNAI 4869, Berlin, Heidelberg (2007).
- Pavel Pech: *Selected topics in geometry with classical vs. computer proving*. World Scientific Publishing Co. Pte. Ltd., Singapore (2007).

  http://books.google.es/books?id=hIb-Vuq16zIC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

- In page 189 of the second, we can find (**Section 8.1**):

  "**Theorem 8.1.** A regular skew pentagon *ABCDE* in the Euclidean space E^3 is given. Then *ABCDE* is a planar pentagon."

Radical_Pech.MWS

```
> GB1:=Basis( J , plex(b1,b2,c1,c2,c3,d1,d2,d3) );
```

$$GB1 := [d3^2,\ 5 - 20\,d2^2 + 16\,d2^4,\ -3 + 4\,d2^2 + 2\,d1,\ c3,\ 2\,d2 - 4\,d2^3 + c2,\ -1 + 2\,c1,\ b2 - d2,\ 1 - 4\,d2^2 + 2\,b1]$$

```
> GB2:=Basis( L , plex(b1,b2,c1,c2,c3,d1,d2,d3) );
```

$$GB2 := [d3^3,\ 5 - 14\,d3^2 - 20\,d2^2 + 24\,d2^2\,d3^2 + 16\,d2^4,\ -3 + 3\,d3^2 + 4\,d2^2 + 2\,d1,\ d3^2 - 2\,d2^2\,d3^2 + c3\,d3,\ -d3^2 + c3^2,\ 10\,d2 - 15\,d2\,d3^2 - 20\,d2^3 - 4\,d2^3\,d3^2 + 5\,c2,\ -1 + 2\,c1,\ -5\,d2 - 10\,d2\,d3^2 + 8\,d2^3\,d3^2 + 5\,b2,\ 1 - 3\,d3^2 - 4\,d2^2 + 2\,b1]$$

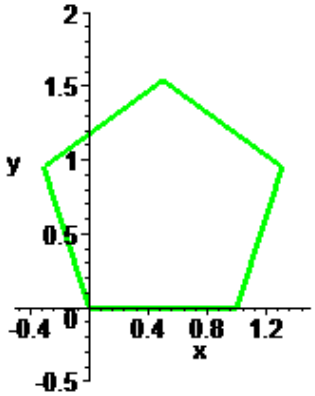
What holds is not:

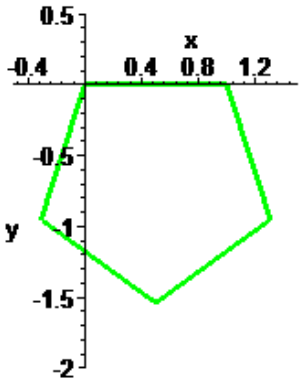
$$GB(<hypothesis>) = GB(<hypothesis,thesis>)$$

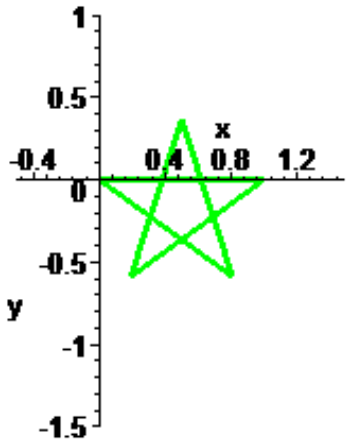
but:

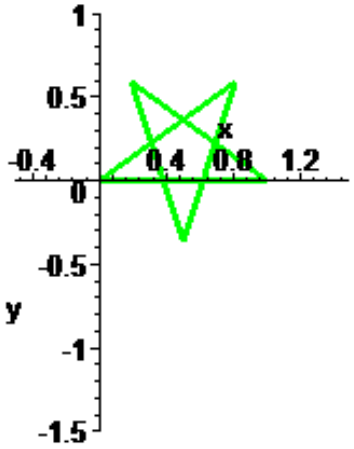
$$GB(<hypothesis>) = GB(<hypothesis,thesis^2>)$$

Looking for explicit solutions with Maple's command: allvalues( );









Is Pech's example (a 3D one) somehow "special" or "unique"?

5 DESIGNING OTHER COUNTEREXAMPLES

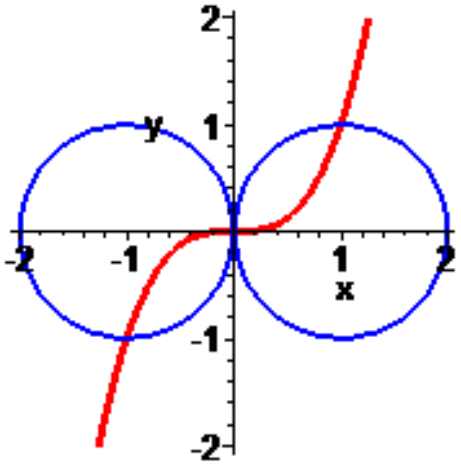
Is Pech's example (a 3D one) somehow "special" or "unique"?

The answer is NO

The idea is to use a kind of "reverse engineering'" to easily find examples of theorems where to check the radical membership is required. It is enough to construct a hypotheses ideal such that the ideal of its variety is not itself and an adequate thesis polynomial.

- 1st Counterexample: Radical_circfscub.MWS

Theorem: The intersection point of the circles of centers (1,0) and (-1,0) and radius 1 lie on the cubic y= x^3.




```
> thesis:=y-x^3:
> GB1:=Basis( [ (x-1)^2+y^2-1 , (x+1)^2+y^2-1], plex(x,y) );
> GB2:=Basis( [ (x-1)^2+y^2-1 , (x+1)^2+y^2-1, thesis ], plex(x,y) );
```

$$GB1 := [y^2, x]$$

$$GB2 := [y, x]$$

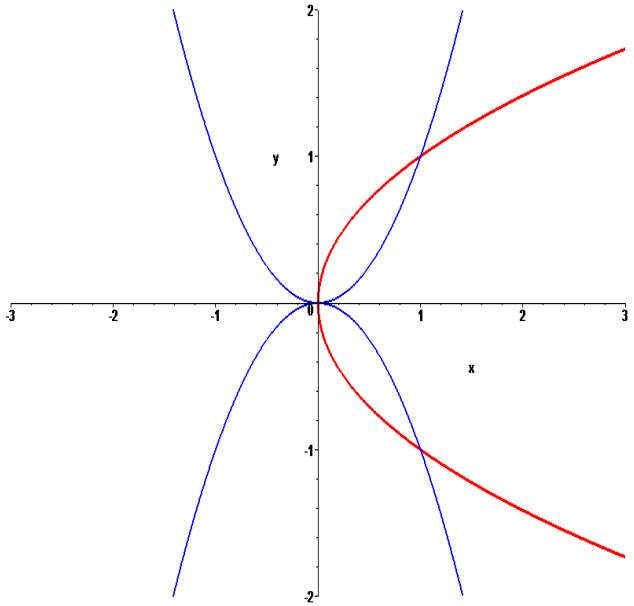
```
> Basis( [ (x-1)^2+y^2-1 , (x+1)^2+y^2-1, 1-w*thesis ], plex(x,y,w) );
```

$$[1]$$

2nd Counterexample:

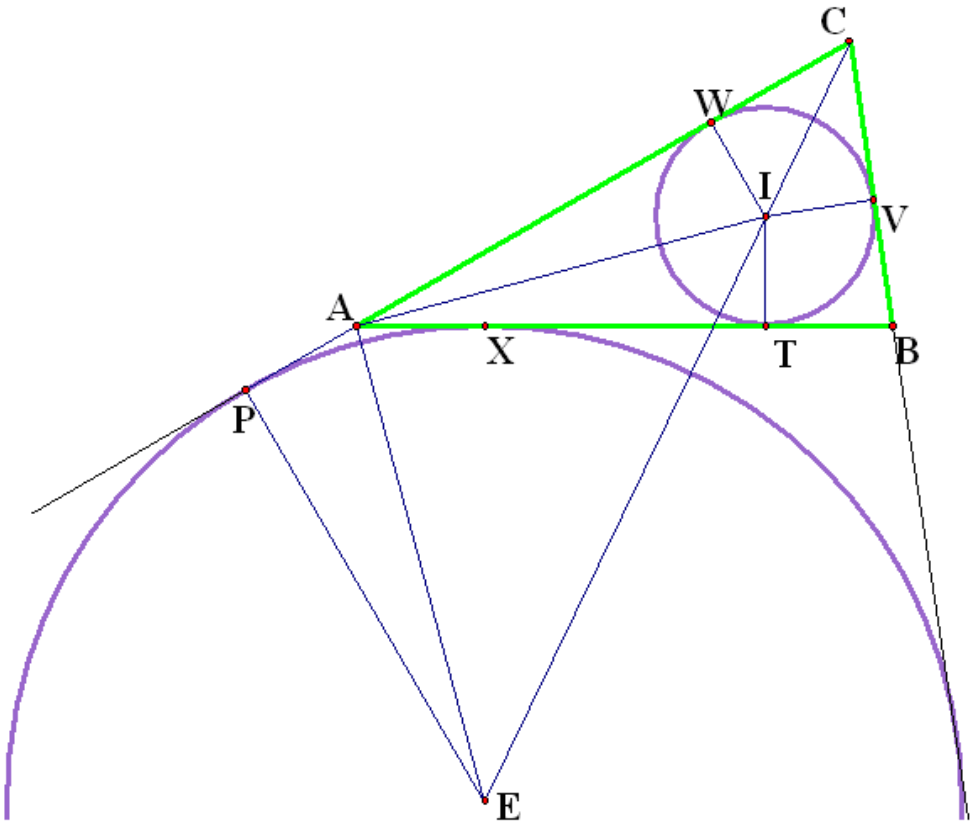
Radical_parabs.MWS

Theorem: The locus of the points of R^2 that are at the same distance of point (0,1/4) and line y=-1/4 and are at the same distance of point (0,-1/4) and line y=1/4 is contained in the locus of the points that are at the same distance of point (1/4,0) and line x=-1/4.



And nontrivial counterexamples can also be found:

Theorem: If *T* and *X* are the tangency points of the inscribed circle and the excribed circle on the side *AB* of triangle *ABC* (respectively), then *dist(A,X)=dist(T,B)*.



5 CONCLUSIONS

Regarding the need for radical membership checking:

- Pavel Pech's regular pentagon example is not an isolated rare case.
- Using a kind of “reverse engineering”' we have shown how to easily find other counterexamples.