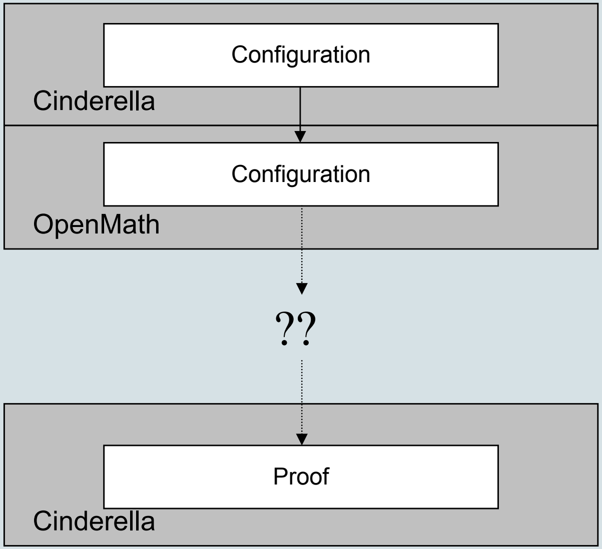
# Proving Statements in Planar Geometry and *Cinderella*

Dan Roozemond

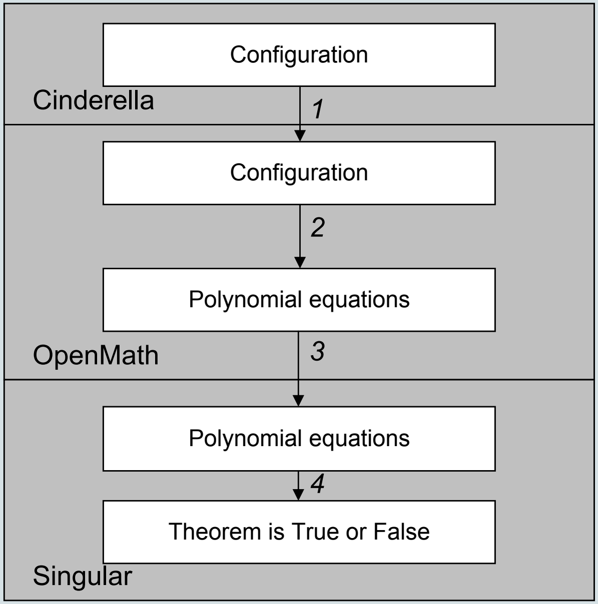
October 2003

# Contents

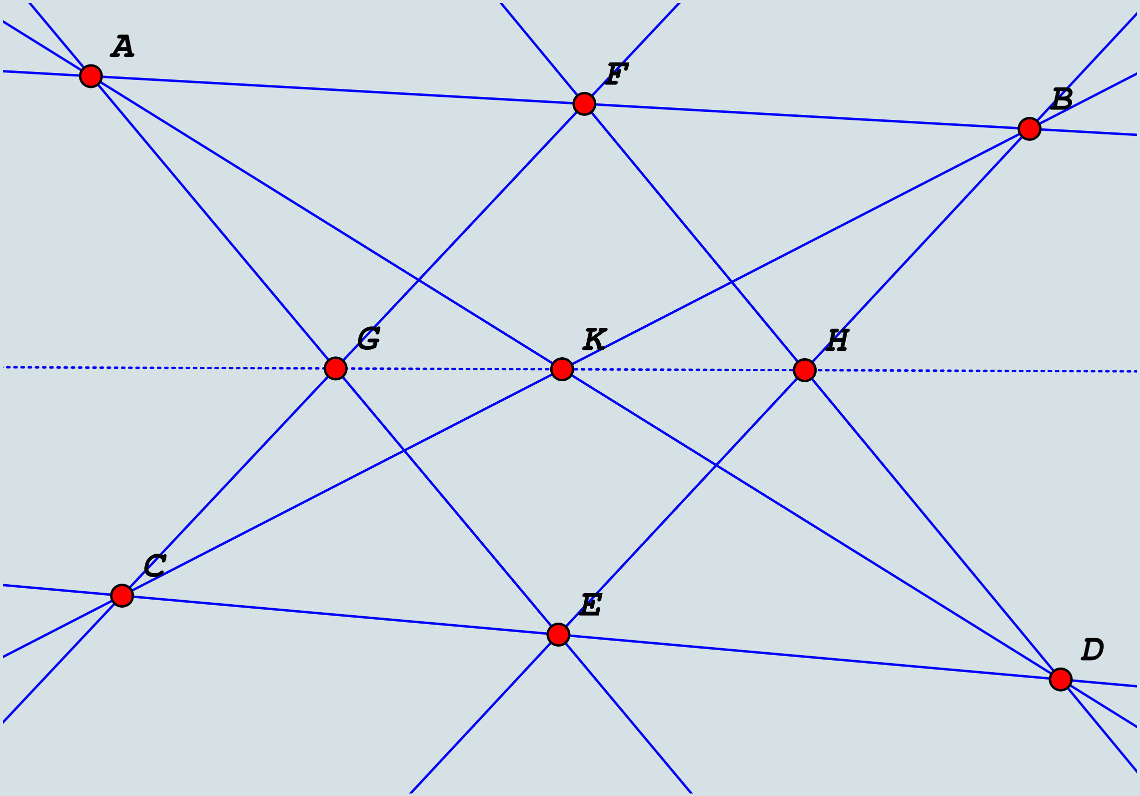
# Introduction - 1



# Introduction - 2



# Cinderella - 1



# Cinderella - 2

- Randomized prover,
- Homogeneous coordinates: $\underline{x} \in (\mathbb{R}^3\{0\})/(\mathbb{R}\{0\})$:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \quad \forall\lambda \in \mathbb{R}, \lambda \neq 0,$$

# Cinderella - 2

- Randomized prover,
- Homogeneous coordinates: $\underline{x} \in (\mathbb{R}^3\{0\})/(\mathbb{R}\{0\})$:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \quad \forall \lambda \in \mathbb{R}, \lambda \neq 0,$$

- $a =$`Join`$(A, B) \Leftrightarrow a = A \times B$,
- $A =$`Meet`$(a, b) \Leftrightarrow A = a \times b$,
- $A$ on $a \Leftrightarrow a.A = 0$,
- $A$, $B$, and $C$ on one line $\Leftrightarrow |ABC| = 0$.

# Gröbner basis - 1

- Work in the *Ring* $\mathbb{Q}[X_1, \ldots, X_l]$,
- *Configuration*: $c_1(\underline{X}), \ldots, c_n(\underline{X})$,
- *Thesis*: $t(\underline{X})$,

$$\text{Thesis holds} \;\Leftrightarrow$$
$$\forall(\underline{X} : c_1(\underline{X}) = \ldots = c_n(\underline{X}) = 0 : t(\underline{X}) = 0),$$

# Gröbner basis - 2

$$\text{Thesis holds} \Leftrightarrow$$
$$\forall(\underline{X} : c_1(\underline{X}) = \ldots = c_n(\underline{X}) = 0 : t(\underline{X}) = 0),$$

- Use the Ideal $I = (c_1, \ldots, c_n) \subseteq \mathbb{Q}[X_1, \ldots, X_l]$,
- Hilbert's Nullstellensatz: Thesis holds *if and only if* $t \in \sqrt{I}$,

# Gröbner basis - 2

$$\text{Thesis holds} \Leftrightarrow$$
$$\forall(\underline{X} : c_1(\underline{X}) = \ldots = c_n(\underline{X}) = 0 : t(\underline{X}) = 0),$$

- Use the Ideal $I = (c_1, \ldots, c_n) \subseteq \mathbb{Q}[X_1, \ldots, X_l]$,
- Hilbert's Nullstellensatz: Thesis holds *if and only if* $t \in \sqrt{I}$,
- Gröbner basis $G = GB(I, tz - 1)$
- $t \in \sqrt{I} \Leftrightarrow$ remainder on division of $1$ by $G$ is $0$,
- Proofs by Extended Gröbner basis algorithm or modules.

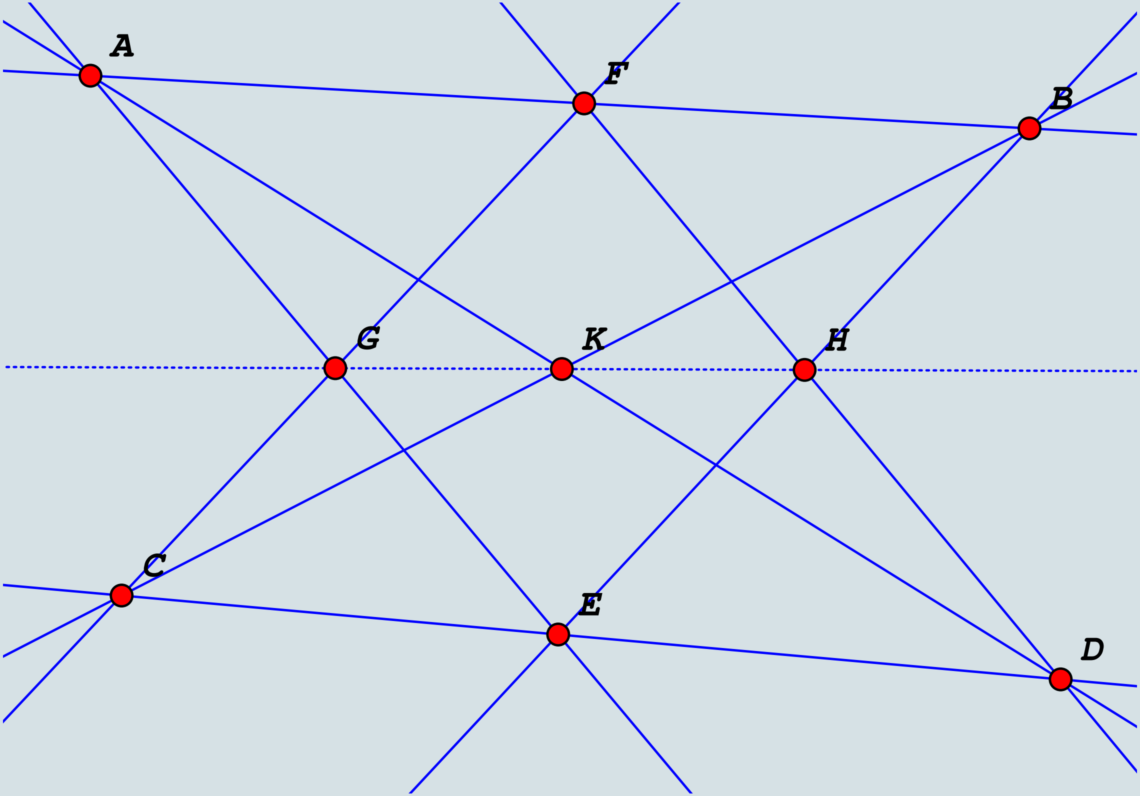
# Gröbner basis - 3: Calculate a Gröbner basis

- Doubly exponential,
- Intermediate results very large,
- Can be optimized in case of homogeneous equations:

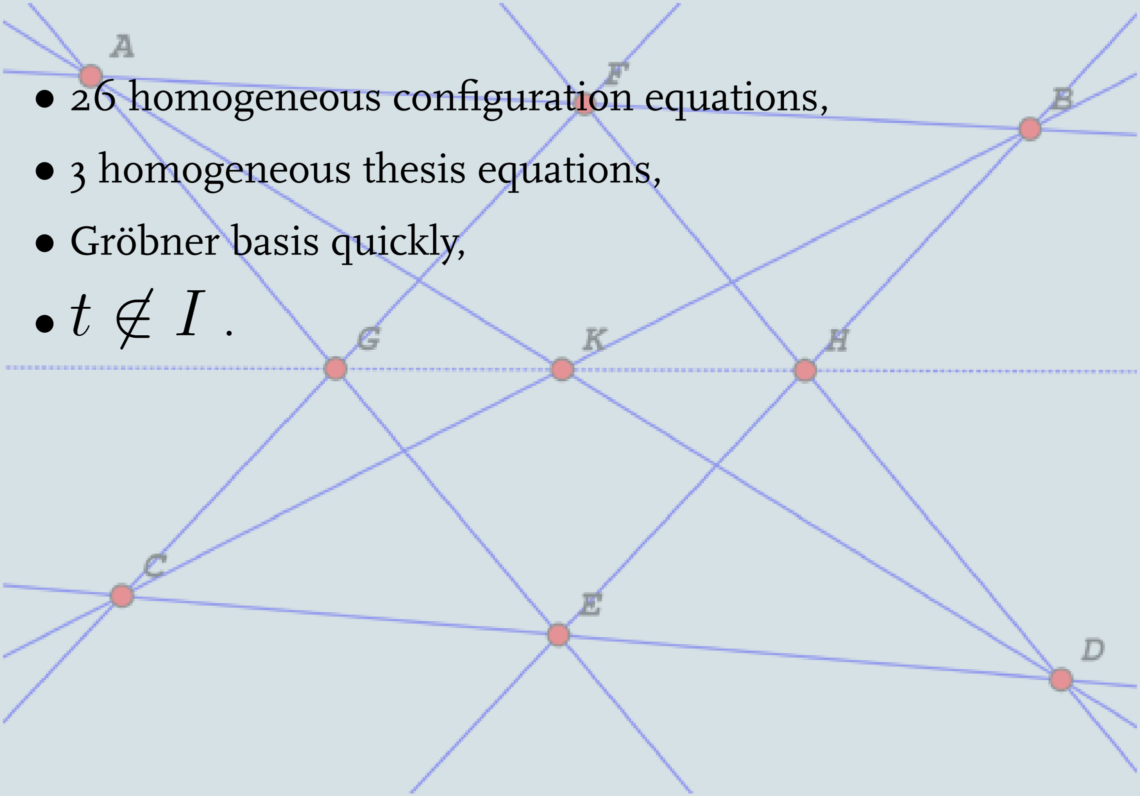
$$A \text{ on } a \Leftrightarrow x_A x_a + y_A y_a + z_A z_a = 0$$

Only consider polynomials of degree $\leq 2$! But limited to $t \in I$.

# Gröbner basis - 4

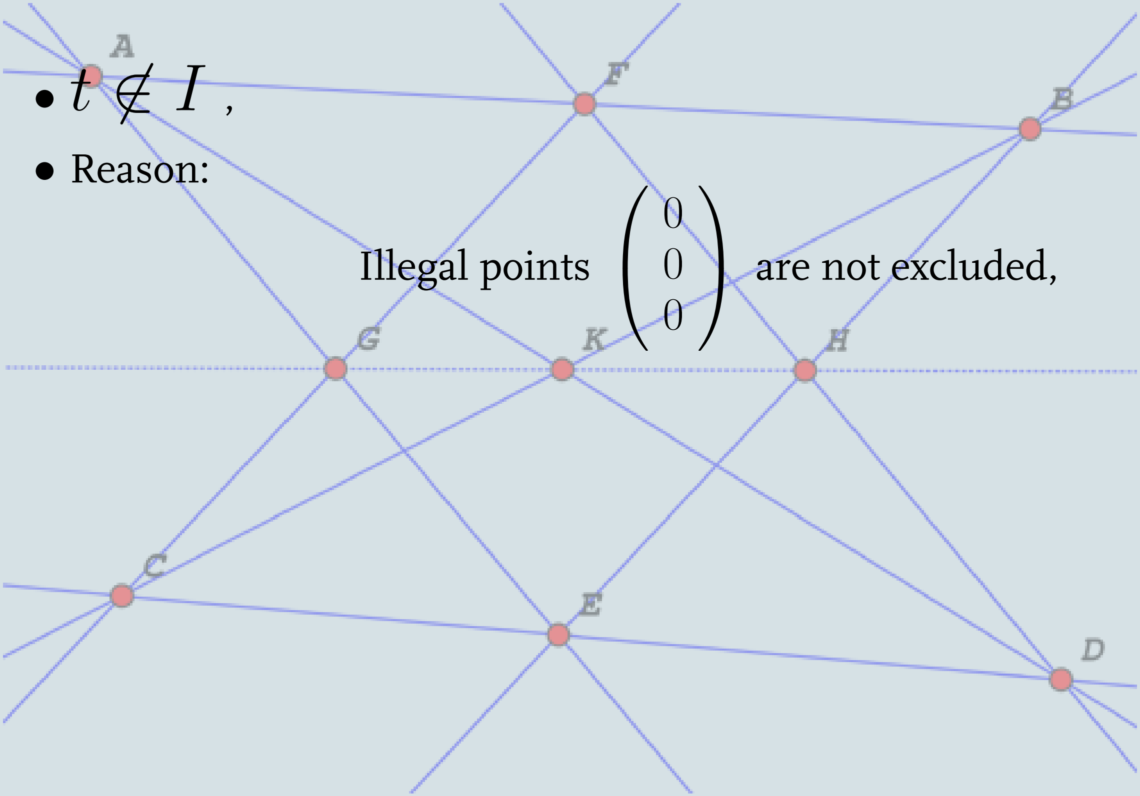


# Gröbner basis - 4




- 26 homogeneous configuration equations,
- 3 homogeneous thesis equations,
- Gröbner basis quickly,
- $t \notin I$ .

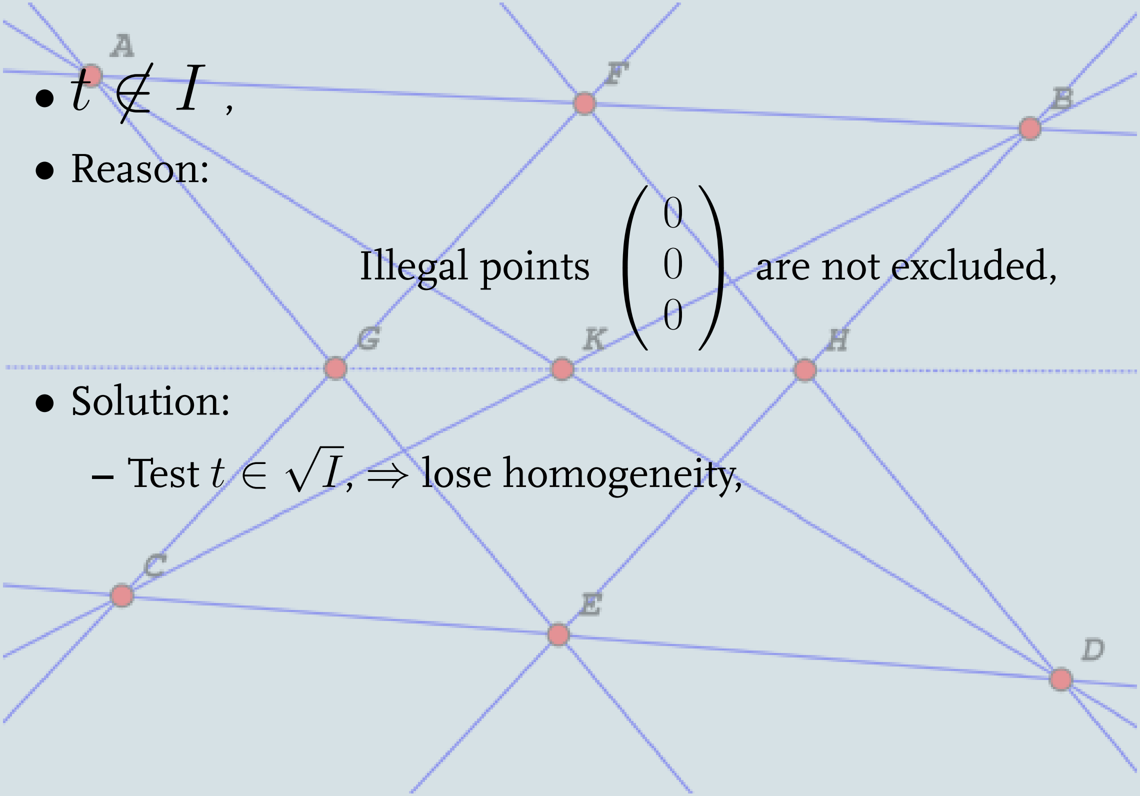
# Gröbner basis - 5




- $t \notin I$ ,
- Reason:

$$\text{Illegal points } \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ are not excluded,}$$

# Gröbner basis - 5

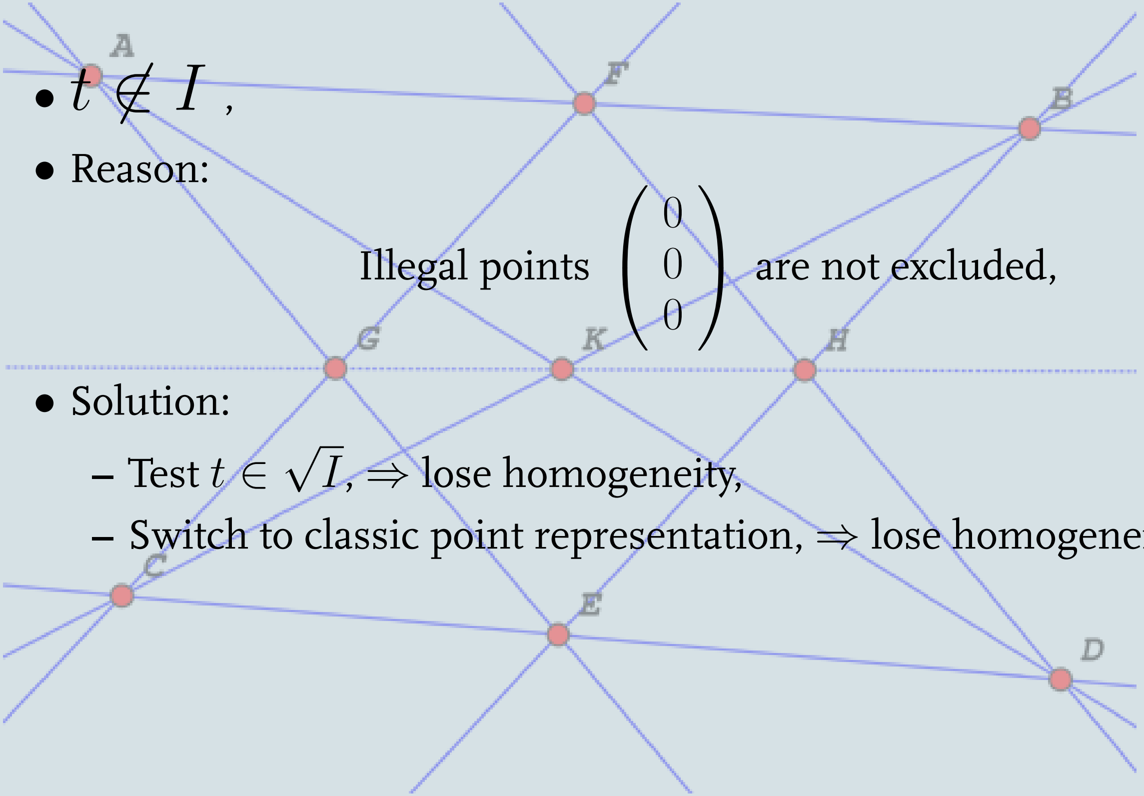



- $t \notin I$ ,
- Reason:

$$\text{Illegal points } \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ are not excluded,}$$

- Solution:
  - Test $t \in \sqrt{I}$, $\Rightarrow$ lose homogeneity,

# Gröbner basis - 5

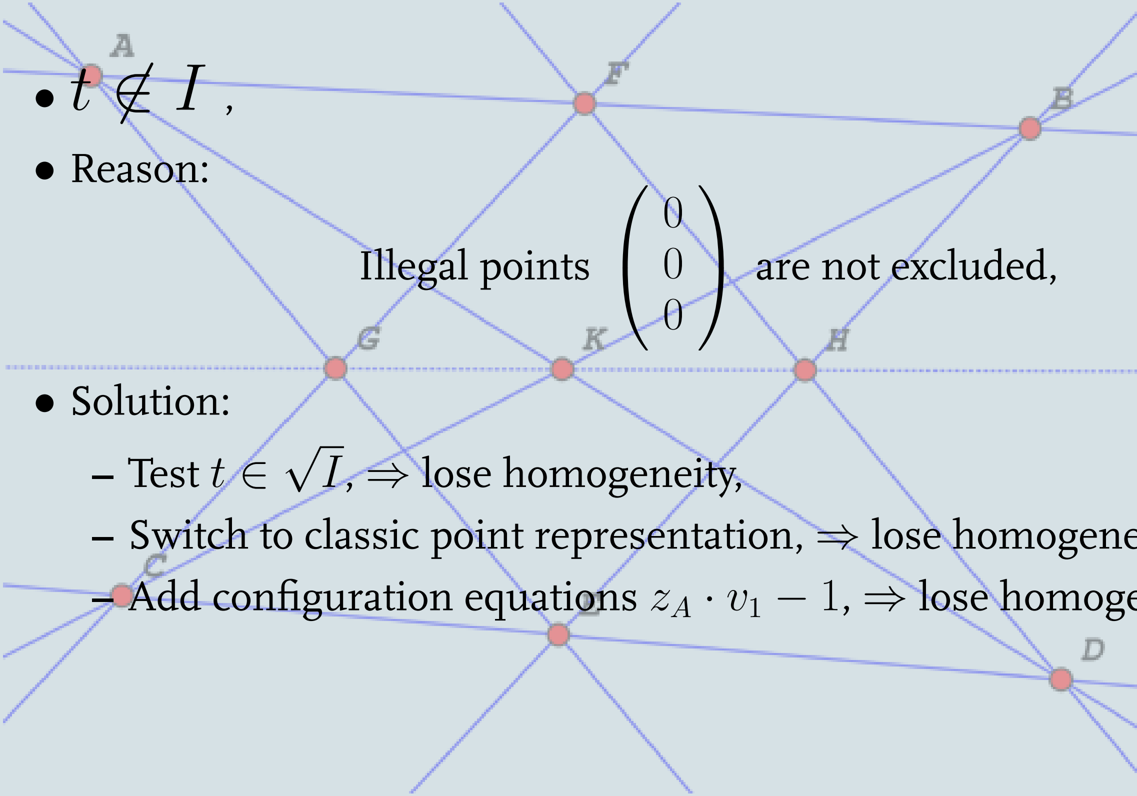



- $t \notin I$ ,
- Reason:

$$\text{Illegal points } \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ are not excluded,}$$

- Solution:
  - Test $t \in \sqrt{I}$, $\Rightarrow$ lose homogeneity,
  - Switch to classic point representation, $\Rightarrow$ lose homogeneity,

# Gröbner basis - 5

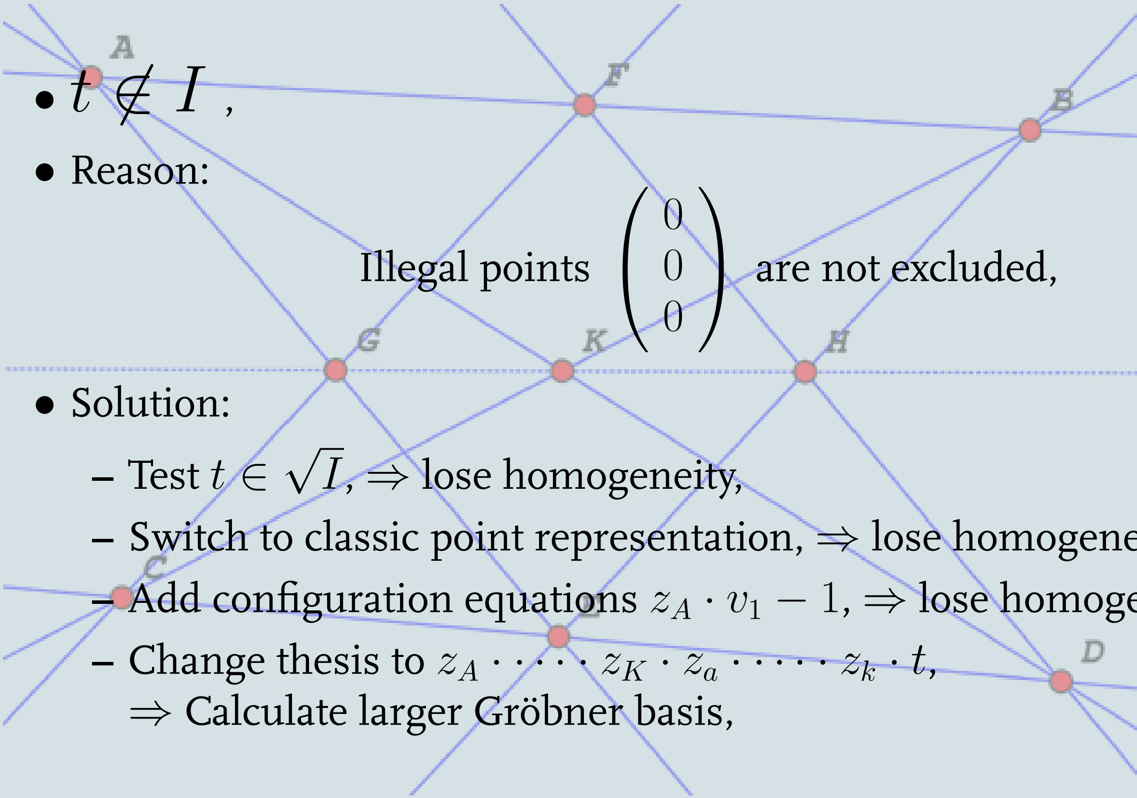



- $t \notin I$ ,
- Reason:

$$\text{Illegal points } \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ are not excluded,}$$

- Solution:
  - Test $t \in \sqrt{I}$, $\Rightarrow$ lose homogeneity,
  - Switch to classic point representation, $\Rightarrow$ lose homogeneity,
  - Add configuration equations $z_A \cdot v_1 - 1$, $\Rightarrow$ lose homogeneity,

# Gröbner basis - 5




- $t \notin I$ ,
- Reason:

$$\text{Illegal points} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{are not excluded,}$$

- Solution:
  - Test $t \in \sqrt{I}$, $\Rightarrow$ lose homogeneity,
  - Switch to classic point representation, $\Rightarrow$ lose homogeneity,
  - Add configuration equations $z_A \cdot v_1 - 1$, $\Rightarrow$ lose homogeneity,
  - Change thesis to $z_A \cdot \cdots \cdot z_K \cdot z_a \cdot \cdots \cdot z_k \cdot t$,
    $\Rightarrow$ Calculate larger Gröbner basis,

Gröbner bases are *not* suitable here

# Brackets - 1

- Assertions invariant under projective transformations,
- Calculate with *brackets*:

$$[ABC] := \begin{vmatrix} x_A & x_B & x_C \\ y_A & y_B & y_C \\ z_A & z_B & z_C \end{vmatrix}$$

- For example: $A$, $B$, and $C$ collinear $\Leftrightarrow$ $[ABC] = 0$.

# Brackets - 2

- $A$, $B$, and $C$ collinear: $h(A, B, C)$,
- Translate to brackets:

$$[ABC] = 0 \Leftrightarrow [ABD][ACE] = [ABE][ACD],$$

- Proof: $4$-linear alternating form on $\{2, 3, 4, 5\}$:

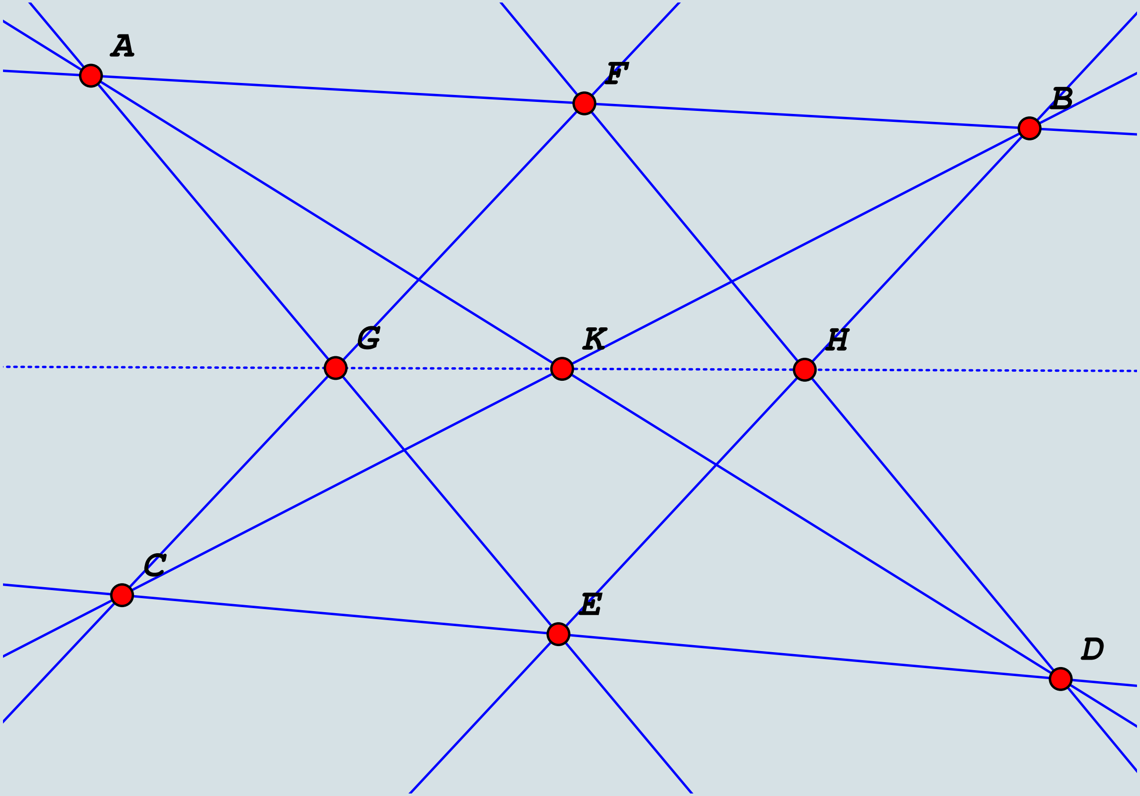
$$[ABC][ADE] - [ABD][ACE] + [ABE][ACD].$$

# Brackets - 3

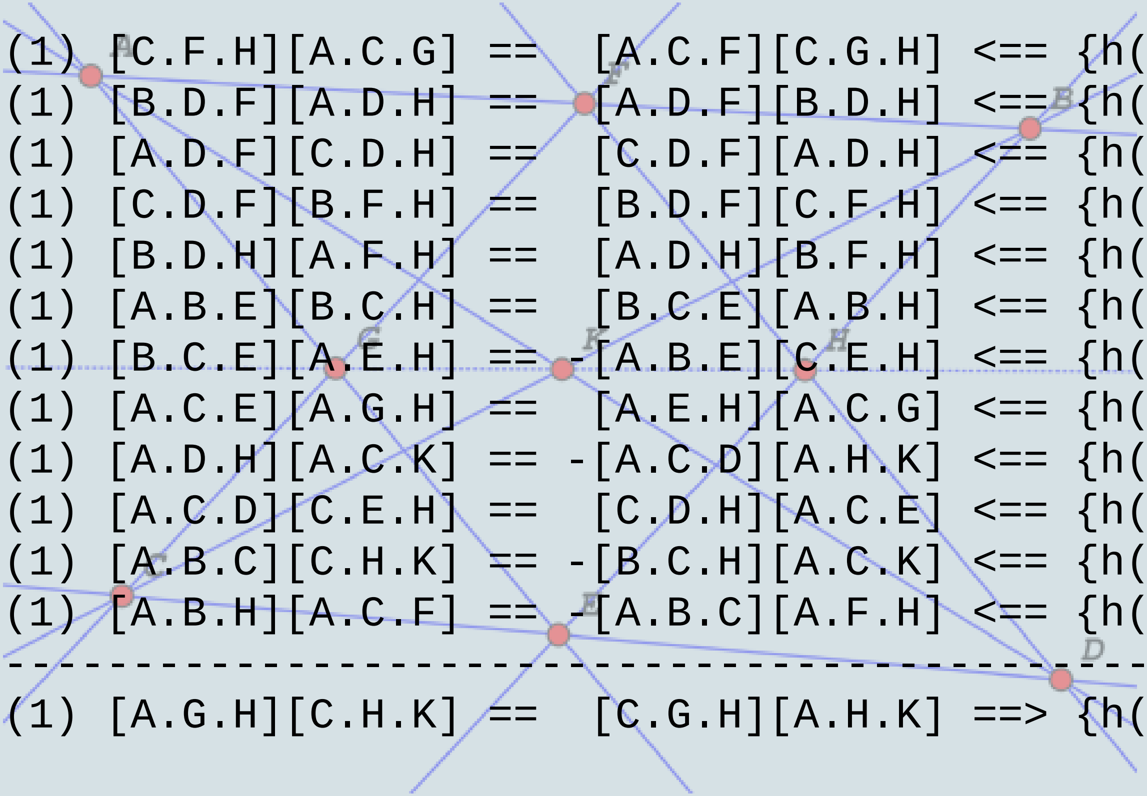
$$\begin{array}{lrcl} \text{Configuration:} & [.1.][.2.] & = & [.3.][.4.] \\ & [\ldots][\ldots] & = & [\ldots][\ldots] \\ & \vdots & \vdots & \vdots \\ & [\ldots][\ldots] & = & [\ldots][\ldots] \\ & & & \\ \text{Thesis:} & [\ldots][\ldots] & = & [\ldots][\ldots] \end{array}$$

- *Might* be solved by a system of *linear* equations....

# Pappos' Theorem



# Pappos' Theorem




```
(1) [C.F.H][A.C.G] ==  [A.C.F][C.G.H] <== {h(C, F, G)}
(1) [B.D.F][A.D.H] ==  [A.D.F][B.D.H] <== {h(D, F, H)}
(1) [A.D.F][C.D.H] ==  [C.D.F][A.D.H] <== {h(D, F, H)}
(1) [C.D.F][B.F.H] ==  [B.D.F][C.F.H] <== {h(D, F, H)}
(1) [B.D.H][A.F.H] ==  [A.D.H][B.F.H] <== {h(D, F, H)}
(1) [A.B.E][B.C.H] ==  [B.C.E][A.B.H] <== {h(B, E, H)}
(1) [B.C.E][A.E.H] == -[A.B.E][C.E.H] <== {h(B, E, H)}
(1) [A.C.E][A.G.H] ==  [A.E.H][A.C.G] <== {h(A, E, G)}
(1) [A.D.H][A.C.K] == -[A.C.D][A.H.K] <== {h(A, D, K)}
(1) [A.C.D][C.E.H] ==  [C.D.H][A.C.E] <== {h(C, D, E)}
(1) [A.B.C][C.H.K] == -[B.C.H][A.C.K] <== {h(B, C, K)}
(1) [A.B.H][A.C.F] == -[A.B.C][A.F.H] <== {h(A, B, F)}
-----------------------------------------------------
(1) [A.G.H][C.H.K] ==  [C.G.H][A.H.K] ==> {h(G, H, K)}
```

# Brackets - 4

Encode other projective assertions:

- $m((A,B),(C,D),(E,F))$:

$$[ABF][CDE] = [ABE][CDF],$$

- $c(A,B,C,D,E,F)$:

$$[ACE][BDE][ABF][CDF] = [ABE][CDE][ACF][BDF].$$

# Brackets - 5

Advantages:

- **Quick**,

# Brackets - 5

Advantages:

- **Quick**,
- **Quick**,

# Brackets - 5

Advantages:

- **Quick**,
- **Quick**,
- Implicit non-degeneracy conditions,

# Brackets - 5

Advantages:

- **Quick**,
- **Quick**,
- Implicit non-degeneracy conditions,
- Easy to check.

# Brackets - 5

Advantages:

- **Quick**,
- **Quick**,
- Implicit non-degeneracy conditions,
- Easy to check.

Disadvantages:

- Not common knowledge,

# Brackets - 5

Advantages:

- **Quick**,
- **Quick**,
- Implicit non-degeneracy conditions,
- Easy to check.

Disadvantages:

- Not common knowledge,
- Not able to proof a theorem false,

# Brackets - 5

Advantages:

- **Quick**,
- **Quick**,
- Implicit non-degeneracy conditions,
- Easy to check.

Disadvantages:

- Not common knowledge,
- Not able to proof a theorem false,
- Only projective geometry.

# Brackets - 6

Introduce 'complex numbers'

$$I := \begin{pmatrix} 1 \\ i \\ 0 \end{pmatrix} \text{ and } J := \begin{pmatrix} 1 \\ -i \\ 0 \end{pmatrix},$$

# Brackets - 6

Introduce ‘complex numbers’

$$I := \begin{pmatrix} 1 \\ i \\ 0 \end{pmatrix} \text{ and } J := \begin{pmatrix} 1 \\ -i \\ 0 \end{pmatrix},$$

For a point $A$:

$$A = \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \text{ define } z_A := x + iy,$$

# Brackets - 6

Introduce ‘complex numbers’

$$I := \begin{pmatrix} 1 \\ i \\ 0 \end{pmatrix} \text{ and } J := \begin{pmatrix} 1 \\ -i \\ 0 \end{pmatrix},$$

For a point $A$:

$$A = \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \text{ define } z_A := x + iy,$$

then we have

$$[ABI] = z_A - z_B \text{ and } [ABJ] = \overline{z_A - z_B}.$$

# Brackets - 7

Sometimes, we can encode circles, parallel lines and perpendicular lines.

- $ci(A, B, C, D)$:

$$[ACI][BDI][ABJ][CDJ] = [ABI][CDI][ACJ][BDJ],$$

- $par((A, B), (C, D))$:

$$m((A, B), (C, D), (I, J)),$$

- $perp((A, B), (A, C))$:

$$[ABI][ACJ] = -[ABJ][ACI].$$

# Brackets - 7

Sometimes, we can encode circles, parallel lines and perpendicular lines.

- $ci(A, B, C, D)$:

$$[ACI][BDI][ABJ][CDJ] = [ABI][CDI][ACJ][BDJ],$$

$$[ACE][BDE][ABF][CDF] = [ABE][CDE][ACF][BDF],$$

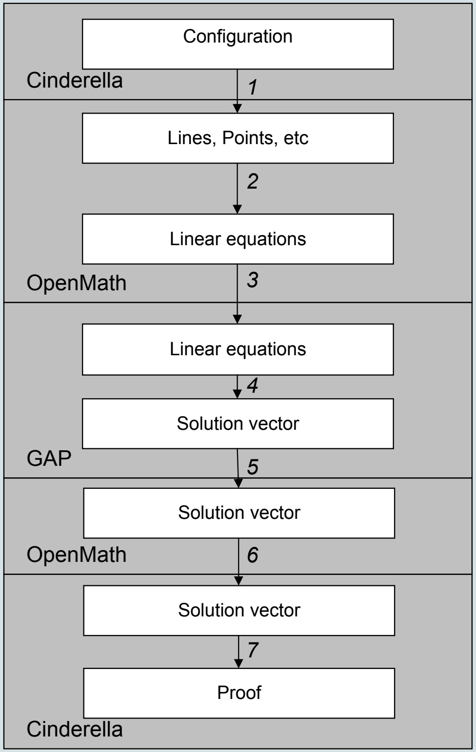
- $par((A, B), (C, D))$:

$$m((A, B), (C, D), (I, J)),$$

- $perp((A, B), (A, C))$:

$$[ABI][ACJ] = -[ABJ][ACI].$$

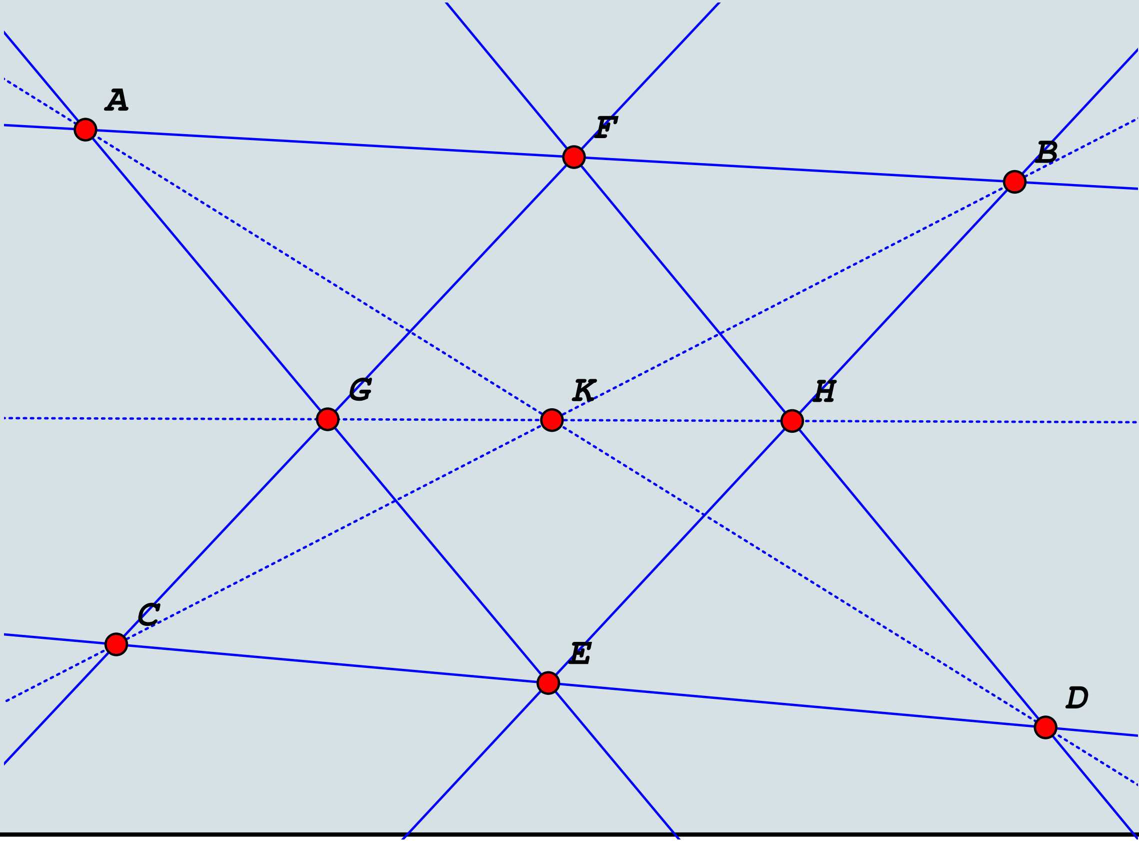
# On the implementation - 1



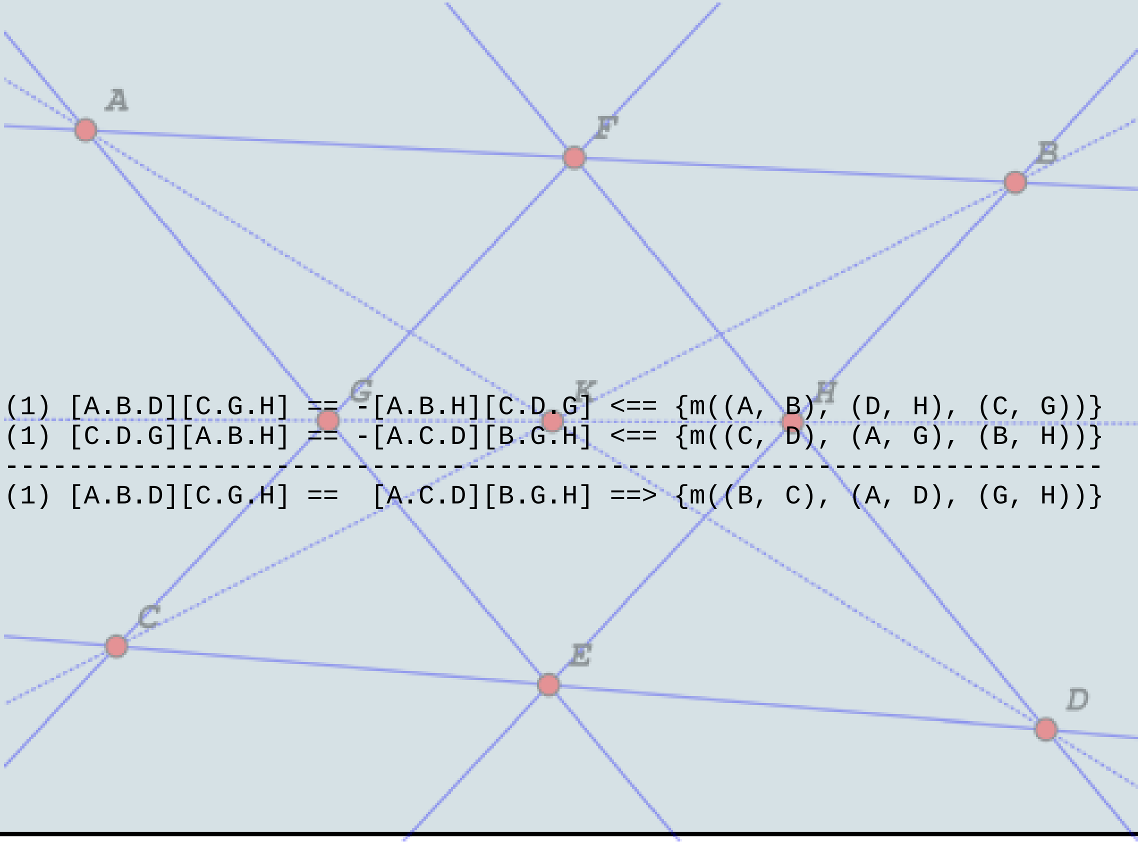
# On the implementation - 2

```
<OMA>
  <OMS name="line" cd="plangeo1"/>
  <OMV name="a"/>
  <OMA>
    <OMS name="incident" cd="plangeo1"/>
    <OMV name="a"/>
    <OMV name="A"/>
  </OMA>
  <OMA>
    <OMS name="incident" cd="plangeo1"/>
    <OMV name="a"/>
    <OMV name="B"/>
  </OMA>
</OMA>
```

# Examples - 1

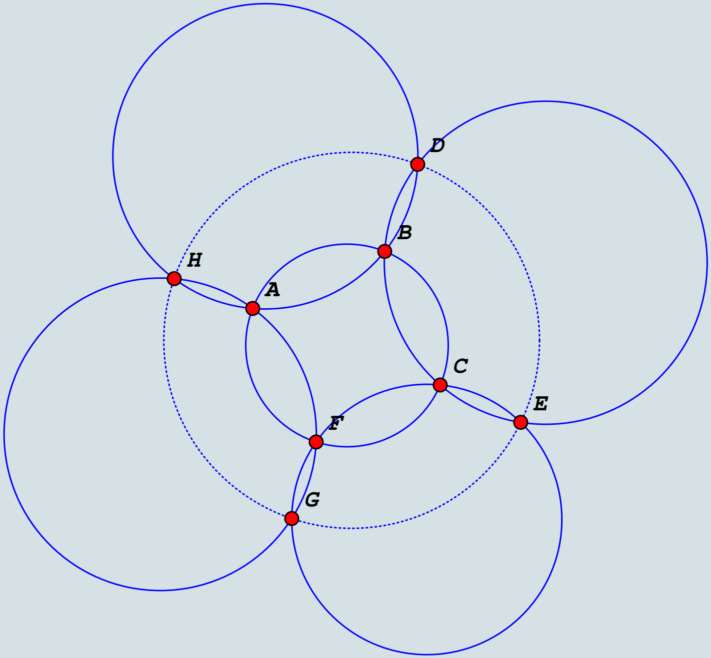


# Examples - 1



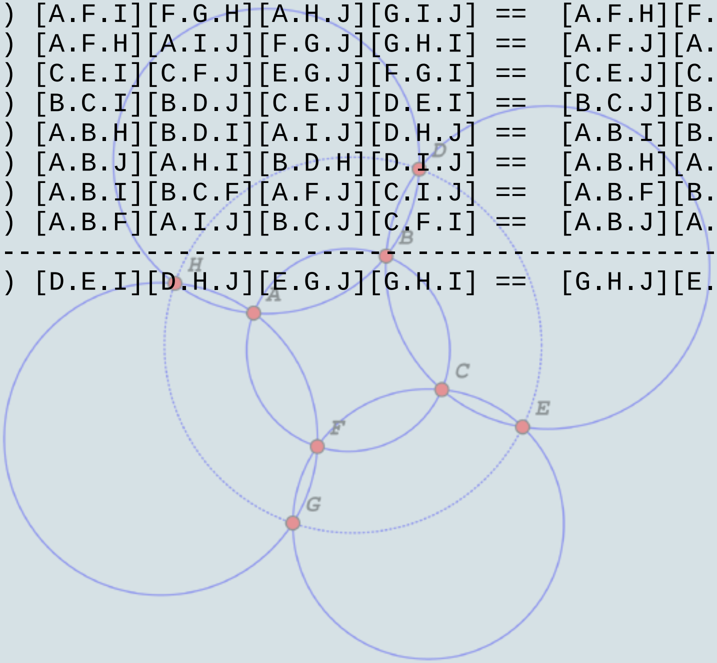

```
(1) [A.B.D][C.G.H] == -[A.B.H][C.D.G] <== {m((A, B), (D, H), (C, G))}
(1) [C.D.G][A.B.H] == -[A.C.D][B.G.H] <== {m((C, D), (A, G), (B, H))}
---------------------------------------------------------------------
(1) [A.B.D][C.G.H] ==  [A.C.D][B.G.H] ==> {m((B, C), (A, D), (G, H))}
```

# Examples - 2

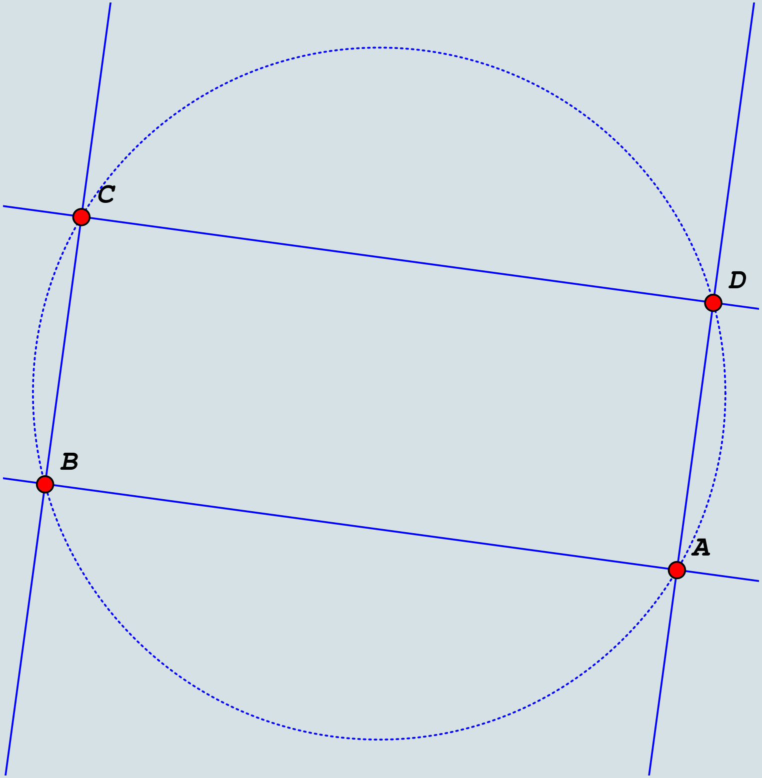


# Examples - 2

```
(1) [A.F.I][F.G.H][A.H.J][G.I.J] ==  [A.F.H][F.G.I][A.I.J][G.H.J] <== {ci(A, F, G, H)}
(1) [A.F.H][A.I.J][F.G.J][G.H.I] ==  [A.F.J][A.H.I][F.G.H][G.I.J] <== {ci(A, F, G, H)}
(1) [C.E.I][C.F.J][E.G.J][F.G.I] ==  [C.E.J][C.F.I][E.G.I][F.G.J] <== {ci(C, E, F, G)}
(1) [B.C.I][B.D.J][C.E.J][D.E.I] ==  [B.C.J][B.D.I][C.E.I][D.E.J] <== {ci(B, C, D, E)}
(1) [A.B.H][B.D.I][A.I.J][D.H.J] ==  [A.B.I][B.D.H][A.H.J][D.I.J] <== {ci(A, B, D, H)}
(1) [A.B.J][A.H.I][B.D.H][D.I.J] ==  [A.B.H][A.I.J][B.D.J][D.H.I] <== {ci(A, B, D, H)}
(1) [A.B.I][B.C.F][A.F.J][C.I.J] ==  [A.B.F][B.C.I][A.I.J][C.F.J] <== {ci(A, B, C, F)}
(1) [A.B.F][A.I.J][B.C.J][C.F.I] ==  [A.B.J][A.F.I][B.C.F][C.I.J] <== {ci(A, B, C, F)}
-------------------------------------------------------------------------------------
(1) [D.E.I][D.H.J][E.G.J][G.H.I] ==  [G.H.J][E.G.I][D.H.I][D.E.J] <== {ci(D, E, G, H)}
```

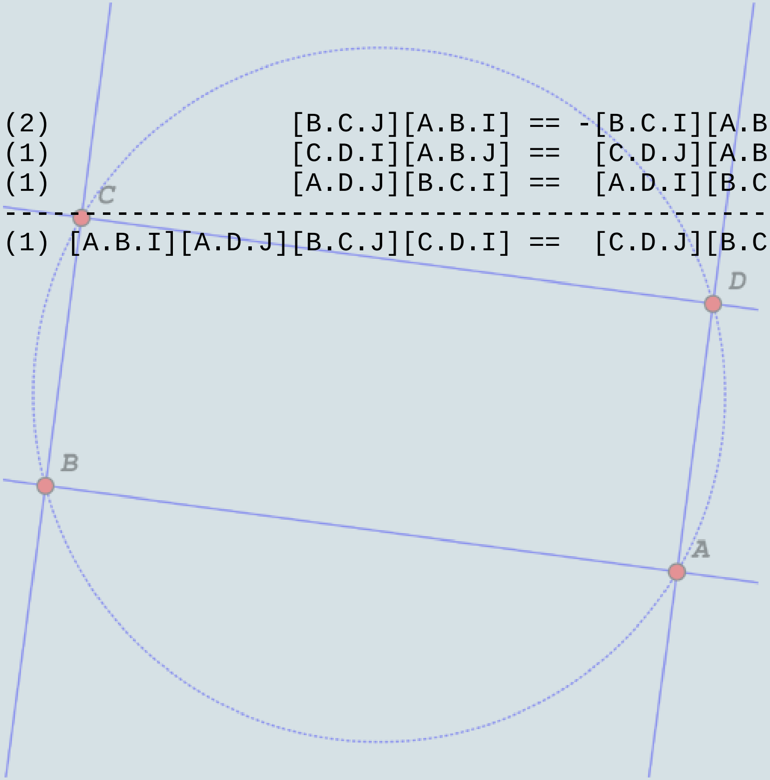


# Examples - 3



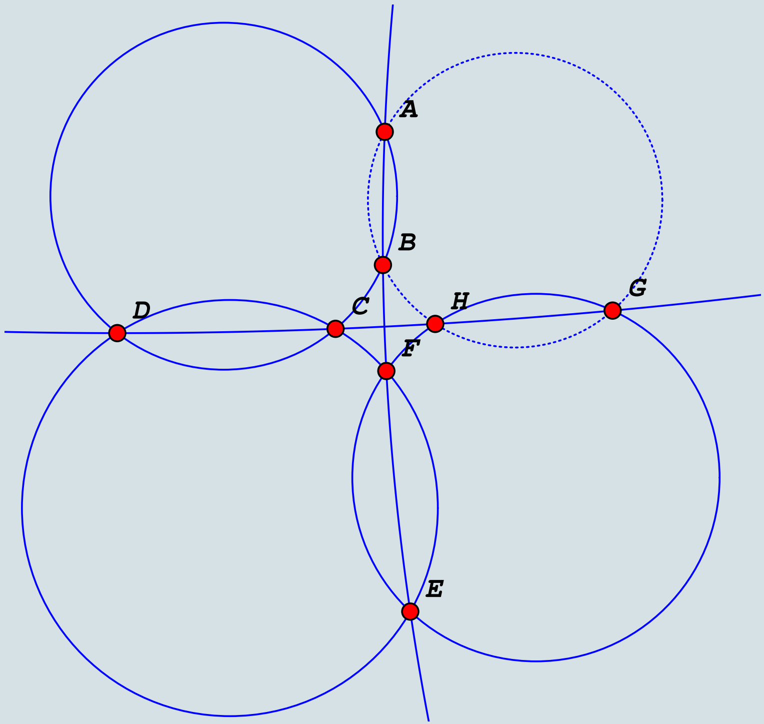
# Examples - 3

```
(2)            [B.C.J][A.B.I] == -[B.C.I][A.B.J]              <== {perp((B, C), (B, A)
(1)            [C.D.I][A.B.J] ==  [C.D.J][A.B.I]              <== {par((C, D), (A, B))
(1)            [A.D.J][B.C.I] ==  [A.D.I][B.C.J]              <== {par((A, D), (B, C))
--------------------------------------------------------------------------------------
(1) [A.B.I][A.D.J][B.C.J][C.D.I] ==  [C.D.J][B.C.I][A.D.I][A.B.J] ==> {ci(A, B, C, D)}
```



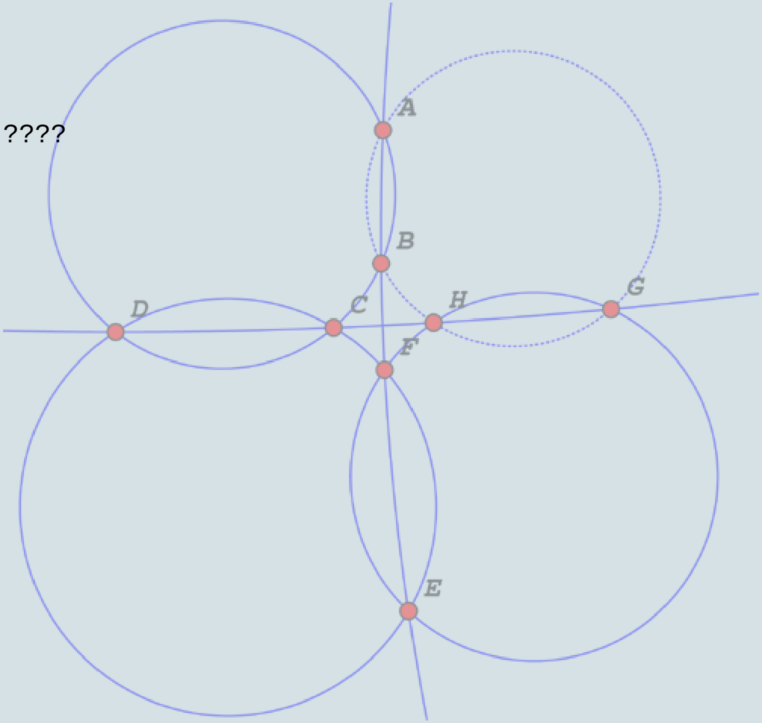
# Demo

# Examples - 4



# Examples - 4

????



# Conclusion

- Gröbner bases $\leftrightarrow$ Brackets
- OpenMath
- Future research

# Questions?