Bachelor's project
"Automatic Geometric Theorem Proving"

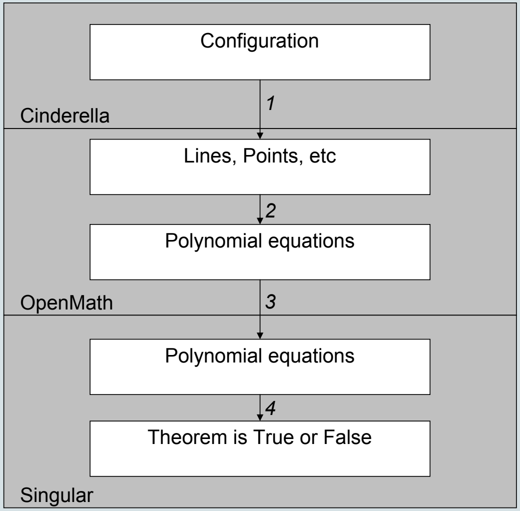
Dan Roozemond

17th July 2003

1. Contents

- Introduction
- How to use Algebra
- Example
- Obtaining a ‘certificate’
- OpenMath
- Demo
- Things to come

2. Introduction



3. How to use Algebra - 1

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

3. How to use Algebra - 1

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

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

3. How to use Algebra - 2

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

- Use the Ideal $I = (c_1, \ldots, c_n) \subseteq \mathbb{Q}[X_1, \ldots, X_l]$,
- If $t \in I$, then:

$$t = f_1 c_1 + \ldots + f_n c_n.$$

3. How to use Algebra - 2

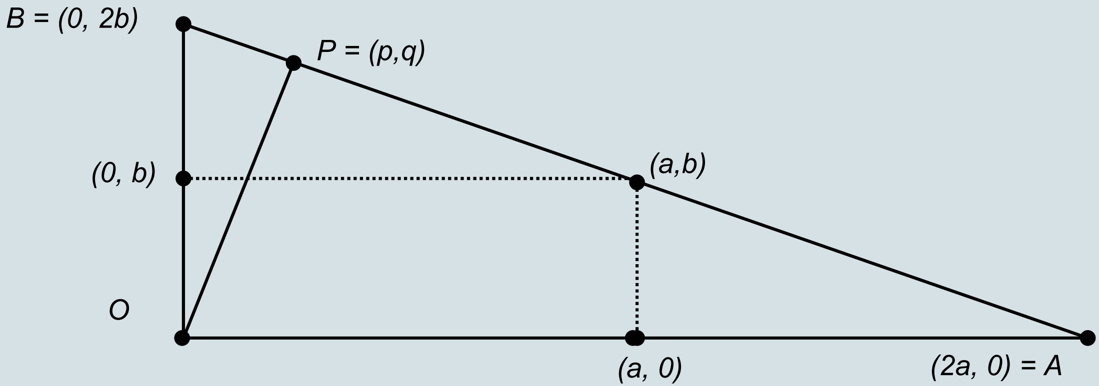
$$\text{Thesis holds} \Leftrightarrow$$
$$\forall(\underline{X} : c_1(\underline{X}) = \ldots = c_n(\underline{X}) = 0 : t(\underline{X}) = 0),$$

- Use the Ideal $I = (c_1, \ldots, c_n) \subseteq \mathbb{Q}[X_1, \ldots, X_l]$,
- If $t \in I$, then:

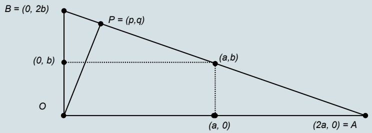
$$t = f_1 c_1 + \ldots + f_n c_n.$$

- Gröbner Basis $G = GB(I)$
- $t \in I \Leftrightarrow$ remainder on division of t by G is 0.

4. Example - Circle Theorem of Appolonius



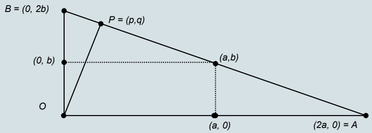
4. Circle Theorem of Appolonius



$$\mathbb{Q}[a, b, m_1, m_2, p, q, s, y]$$

$c_1 = (m_1 - a)^2 + m_2^2 - s^2 \quad (a, 0)$ is on the circle

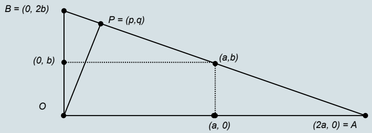
4. Circle Theorem of Appolonius



$$\mathbb{Q}[a, b, m_1, m_2, p, q, s, y]$$

$$c_1 = (m_1 - a)^2 + m_2^2 - s^2 \quad (a, 0) \text{ is on the circle}$$
$$c_2 = (m_1)^2 + (m_2 - b)^2 - s^2 \quad (0, b) \text{ is on the circle}$$

4. Circle Theorem of Appolonius



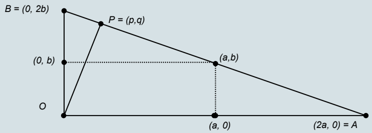
$$\mathbb{Q}[a, b, m_1, m_2, p, q, s, y]$$

$c_1 = (m_1 - a)^2 + m_2^2 - s^2$ — $(a, 0)$ is on the circle

$c_2 = (m_1)^2 + (m_2 - b)^2 - s^2$ — $(0, b)$ is on the circle

$c_3 = (m_1 - a)^2 + (m_2 - b)^2 - s^2$ — (a, b) is on the circle

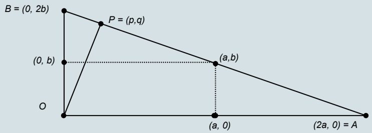
4. Circle Theorem of Appolonius



$$\mathbb{Q}[a, b, m_1, m_2, p, q, s, y]$$

$c_1 = (m_1 - a)^2 + m_2^2 - s^2$	$(a, 0)$ is on the circle
$c_2 = (m_1)^2 + (m_2 - b)^2 - s^2$	$(0, b)$ is on the circle
$c_3 = (m_1 - a)^2 + (m_2 - b)^2 - s^2$	(a, b) is on the circle
$c_4 = -2 \cdot a \cdot p + 2 \cdot b \cdot q$	OP perpendicular AB

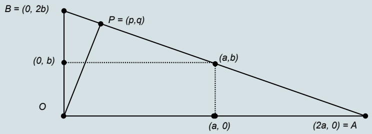
4. Circle Theorem of Appolonius



$\mathbb{Q}[a, b, m_1, m_2, p, q, s, y]$

$c_1 = (m_1 - a)^2 + m_2^2 - s^2$	$(a, 0)$ is on the circle
$c_2 = (m_1)^2 + (m_2 - b)^2 - s^2$	$(0, b)$ is on the circle
$c_3 = (m_1 - a)^2 + (m_2 - b)^2 - s^2$	(a, b) is on the circle
$c_4 = -2 \cdot a \cdot p + 2 \cdot b \cdot q$	OP perpendicular AB
$c_5 = -2 \cdot a \cdot q - 2 \cdot b \cdot p + 2 \cdot a \cdot 2 \cdot b$	P on AB

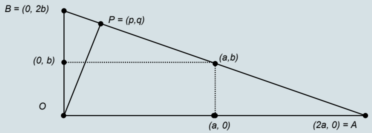
4. Circle Theorem of Appolonius



$$\mathbb{Q}[a, b, m_1, m_2, p, q, s, y]$$

$c_1 = (m_1 - a)^2 + m_2^2 - s^2$	$(a, 0)$ is on the circle
$c_2 = (m_1)^2 + (m_2 - b)^2 - s^2$	$(0, b)$ is on the circle
$c_3 = (m_1 - a)^2 + (m_2 - b)^2 - s^2$	(a, b) is on the circle
$c_4 = -2 \cdot a \cdot p + 2 \cdot b \cdot q$	OP perpendicular AB
$c_5 = -2 \cdot a \cdot q - 2 \cdot b \cdot p + 2 \cdot a \cdot 2 \cdot b$	P on AB
$c_6 = a \cdot b \cdot y - 1$	a, b not equal to zero

4. Circle Theorem of Appolonius



$\mathbb{Q}[a, b, m_1, m_2, p, q, s, y]$

$c_1 = (m_1 - a)^2 + m_2^2 - s^2$	$(a, 0)$ is on the circle
$c_2 = (m_1)^2 + (m_2 - b)^2 - s^2$	$(0, b)$ is on the circle
$c_3 = (m_1 - a)^2 + (m_2 - b)^2 - s^2$	(a, b) is on the circle
$c_4 = -2 \cdot a \cdot p + 2 \cdot b \cdot q$	OP perpendicular AB
$c_5 = -2 \cdot a \cdot q - 2 \cdot b \cdot p + 2 \cdot a \cdot 2 \cdot b$	P on AB
$c_6 = a \cdot b \cdot y - 1$	a, b not equal to zero
$t = (m_1 - p)^2 + (m_2 - q)^2 - s^2$	P is on the circle

4. Circle Theorem of Appolonius

```
> ring r=0,(a,b,m(1..2),p,q,s,y),(c,dp);
> poly c1=(m(1)-a)^2+m(2)^2-s^2;
> poly c2=(m(1))^2+(m(2)-b)^2-s^2;
> poly c3=(m(1)-a)^2+(m(2)-b)^2-s^2;
> poly c4=-2*a*p+2*b*q;
> poly c5=-2*a*q-2*b*p+2*a*2*b;
> poly c6=a*b*y-1;
> poly t=(m(1)-p)^2+(m(2)-q)^2-s^2;
> ideal i=(c1,c2,c3,c4,c5,c6);
> reduce(t,groebner(i));
0
```

5. Obtaining a 'certificate' - 1

- Use the Ideal $I = (c_1, \ldots, c_n) \subseteq \mathbb{Q}[X_1, \ldots, X_l]$,
- If $t \in I$, then:

$$t = f_1 c_1 + \ldots + f_n c_n.$$

5. Obtaining a 'certificate' - 2

Modules:

$$M = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ -1 & 0 & \dots & 0 \\ 0 & -1 & \dots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & -1 \end{pmatrix} \subseteq (\mathbb{Q}[X_1, \dots, X_l])^n.$$

5. Obtaining a ‘certificate’ - 3

$$\begin{pmatrix} c_1 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in M, \quad \text{so} \quad \begin{pmatrix} c_1 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \mod M.$$

5. Obtaining a 'certificate' - 3

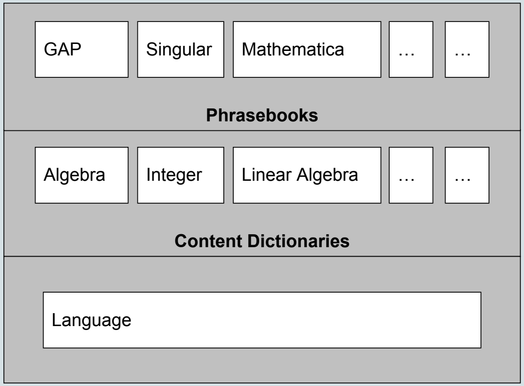
$$\begin{pmatrix} c_1 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in M, \quad \text{so} \quad \begin{pmatrix} c_1 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \mod M.$$

$$\begin{pmatrix} c_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \mod M.$$

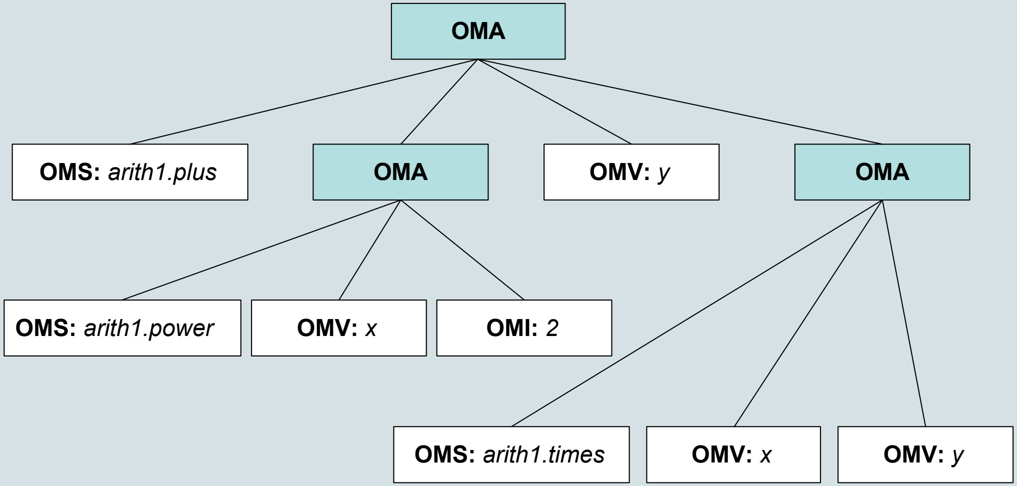
5. Obtaining a ‘certificate’ - 4

$$\begin{pmatrix} t \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} \equiv f_1 \begin{pmatrix} c_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \ldots + f_n \begin{pmatrix} c_n \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \bmod M.$$

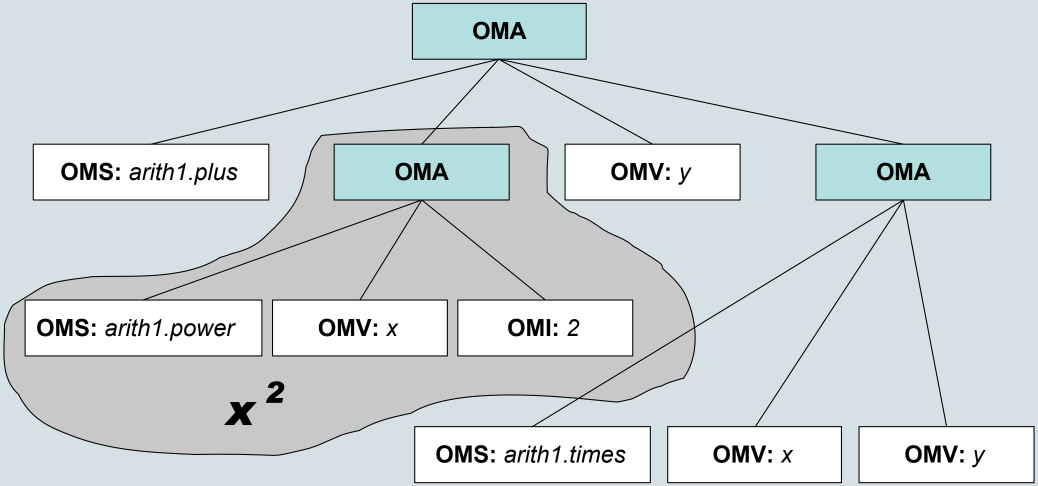
6. OpenMath


GAP
Singular
Mathematica
…
…
Phrasebooks
Algebra
Integer
Linear Algebra
…
…
Content Dictionaries
Language

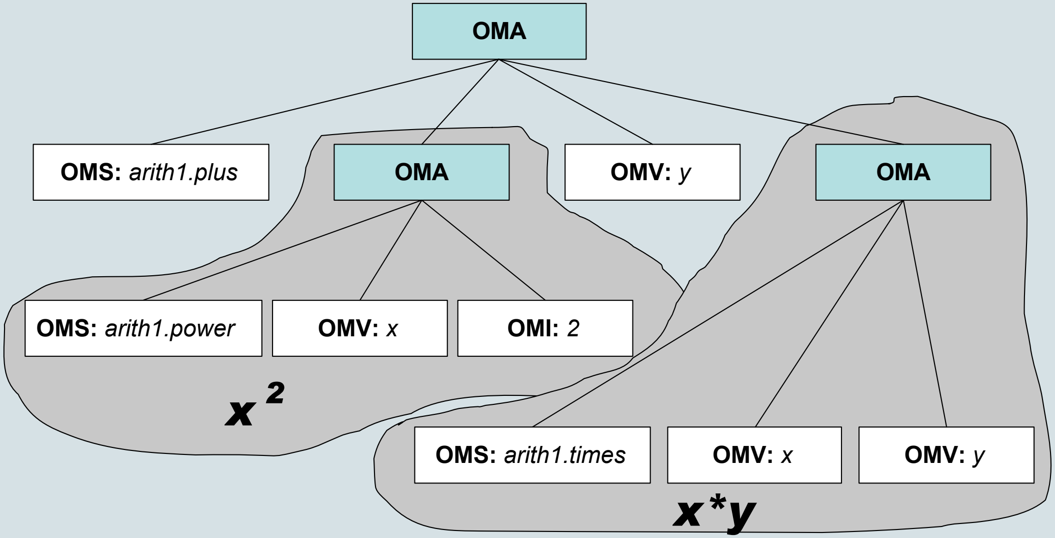
6. OpenMath - Example



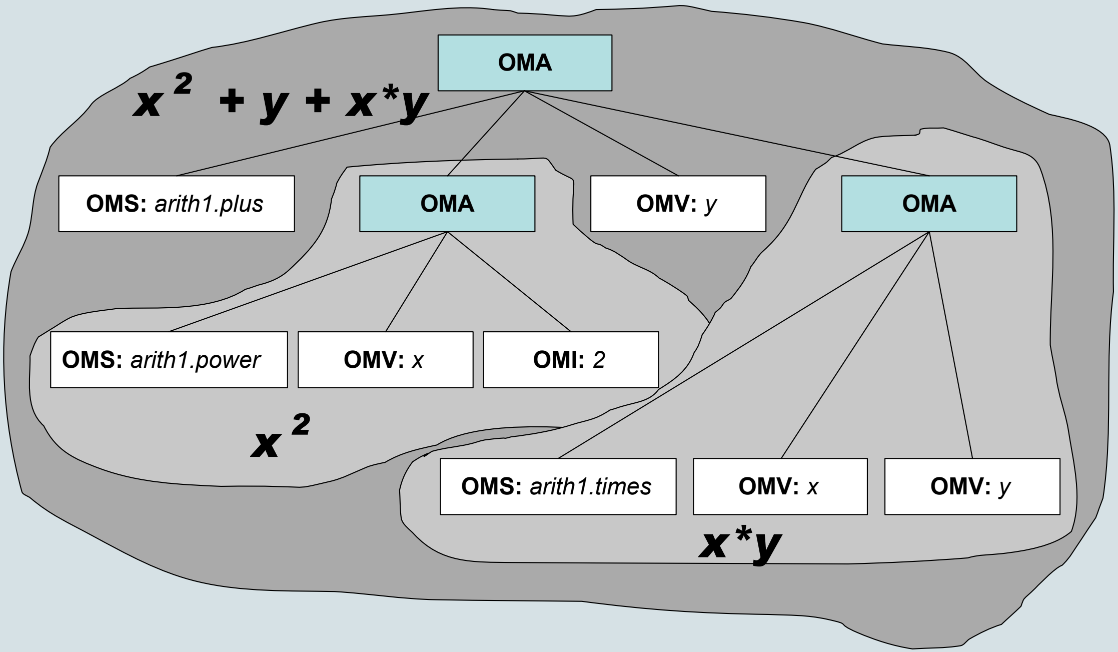
6. OpenMath - Example



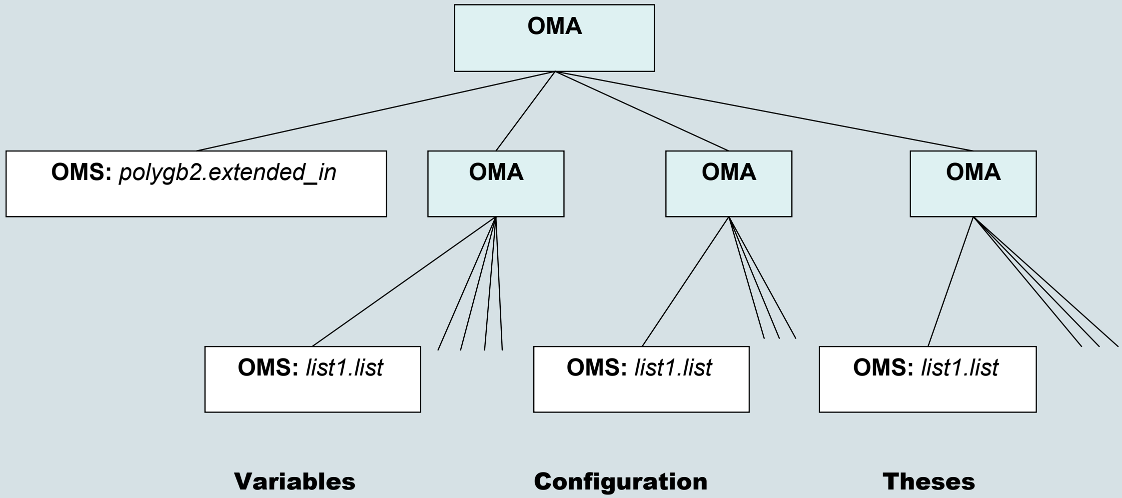
6. OpenMath - Example



6. OpenMath - Example

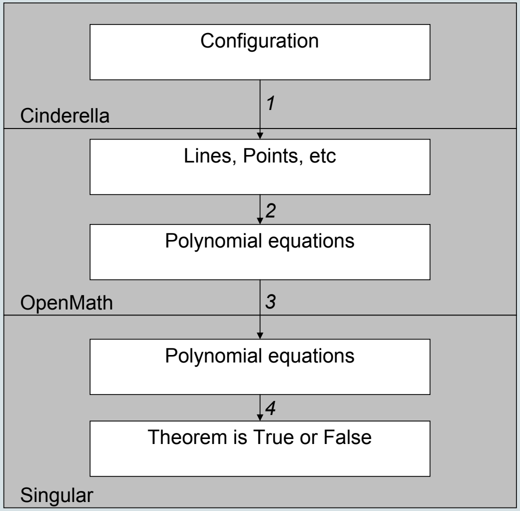


6. OpenMath - Geometric Theorem



7. Demo

8. Things to come



9. Questions?