

M.Sc. projects and JHD

James Davenport

Dept. {Computer,Mathematical} Science{s}
University of Bath, England masjhd@bath.ac.uk

20070202/ MSc

What does JHD do?

What does JHD do?

Mathematics $\stackrel{\text{JHD}}{\Leftrightarrow}$ Computing (1)

What does JHD do?

Mathematics $\stackrel{\text{JHD}}{\Leftrightarrow}$ Computing (1)

- ▶ Cryptography

What does JHD do?

Mathematics $\stackrel{\text{JHD}}{\Leftrightarrow}$ Computing (1)

- ▶ Cryptography
- ▶ Computer Algebra

What does JHD do?

Mathematics $\stackrel{\text{JHD}}{\Leftrightarrow}$ Computing (1)

- ▶ Cryptography
- ▶ Computer Algebra
- ▶ Semantics and Presentation of Mathematics

Cryptography

Using Mathematics to make Computing
“Better” — safer, more useful, more trustworthy

Cryptography

Using Mathematics to make Computing
“Better” — safer, more useful, more trustworthy

- ▶ Cryptography is in use *all* over the Web;

Cryptography

Using Mathematics to make Computing
“Better” — safer, more useful, more trustworthy

- ▶ Cryptography is in use *all* over the Web;
- ▶ Cryptography is in use *all* over the financial world (from cash machines to paying off Lend-Lease);

Cryptography

Using Mathematics to make Computing
“Better” — safer, more useful, more trustworthy

- ▶ Cryptography is in use *all* over the Web;
- ▶ Cryptography is in use *all* over the financial world (from cash machines to paying off Lend-Lease);
- ▶ JHD was on the team that broke the Federal Reserve Bank code in 1982.

Computer Algebra

Using Computing to do bigger Mathematics

Computer Algebra

Using Computing to do bigger Mathematics

- ▶ Computer algebra was a vital part of landing man on the moon (where will it be in two years time?);

Computer Algebra

Using Computing to do bigger Mathematics

- ▶ Computer algebra was a vital part of landing man on the moon (where will it be in two years time?);
- ▶ Also the start of Ramadan — “L’imam attend la lune à 05:48 après-demain”;

Computer Algebra

Using Computing to do bigger Mathematics

- ▶ Computer algebra was a vital part of landing man on the moon (where will it be in two years time?);
- ▶ Also the start of Ramadan — “L'imam attend la lune à 05:48 après-demain”;
- ▶ Also image compression (a French patent contains a 50MB polynomial);

Computer Algebra

Using Computing to do bigger Mathematics

- ▶ Computer algebra was a vital part of landing man on the moon (where will it be in two years time?);
- ▶ Also the start of Ramadan — “L’imam attend la lune à 05:48 après-demain”;
- ▶ Also image compression (a French patent contains a 50MB polynomial);
- ▶ Also enzyme kinetics — “is unknown” $\xRightarrow{\text{Reduce}}$ 20 seconds.

Mathematical Semantics and Presentation

Mathematical Semantics and Presentation

- ▶ What does it look like?

Mathematical Semantics and Presentation

- ▶ What does it look like?
- ▶ What does it mean?

What does it look like?

What does it look like?

- ▶ \LaTeX — as in these slides
 $2xy \ 2xy$

Or, better,

```
<mrow> <mn>2</mn> <mo>&InvisibleTimes;</mo>  
      <mi>x</mi> <mo>&InvisibleTimes;</mo>  
      <mi>y</mi>  
</mrow>
```

What does it look like?

- ▶ \LaTeX — as in these slides

$2xy$ $2xy$

- ▶ MathML (Presentation) — www.w3.org/Math

```
<mrow> <mn>2</mn> <mi>x</mi> <mi>y</mi>
```

Or, better,

```
<mrow> <mn>2</mn> <mo>&InvisibleTimes;</mo>
      <mi>x</mi> <mo>&InvisibleTimes;</mo>
      <mi>y</mi>
</mrow>
```

What does it mean?

OpenMath www.openmath.org

```
<OMA>  
  <OMS name="times" cd="arith1"/>  
  <OMI>2</OMI>  
  <OMV name="x"/>  
  <OMV name="y"/>  
</OMA>
```

Relate the Two

OpenMath \Rightarrow MathML

Relate the Two

OpenMath \Rightarrow MathML

Allowing for

Relate the Two

OpenMath \Rightarrow MathML

Allowing for

- ▶ Linguistic variants: $(0, 1]$ versus $]0, 1]$?

In an extensible way.

Relate the Two

OpenMath \Rightarrow MathML

Allowing for

- ▶ Linguistic variants: $(0, 1]$ versus $]0, 1]$?
- ▶ Subject variants: i or j ;

In an extensible way.

Relate the Two

OpenMath \Rightarrow MathML

Allowing for

- ▶ Linguistic variants: $(0, 1]$ versus $]0, 1]$?
- ▶ Subject variants: i or j ;
- ▶ Personal variants xy or $x \times y$ or $x \cdot y$

In an extensible way.

Relate the Two

OpenMath \Rightarrow MathML

Allowing for

- ▶ Linguistic variants: $(0, 1]$ versus $]0, 1]$?
- ▶ Subject variants: i or j ;
- ▶ Personal variants xy or $x \times y$ or $x \cdot y$
- ▶ Reasonableness of presentation

In an extensible way.