Évaluation AERES, Janvier 2014 Joris van der Hoeven

AMIB. **Varna**, GenRGenS, ESBTL, DiMoVo, VorScore

CRYPTO. Mpc, Mpfrcx, ECPP, SEA, TIFA, **Cado-NFS**, **Mathemagix**, Decoding

MAX. **Mathemagix**, **TeXmacs**

PARSIFAL. **Abella**, Bedwyr, Profound, TLAPS, Psyche

SYSMO. **Altarica**, **Xfta**

TYPICAL. Coq, Deducti, SSReflect

But ANR CADO. Fournir une implantation de référence complète de l'algorithme de factorisation d'entiers NFS (crible algébrique), qui permet de tester des idées nouvelles (sélection polynomiale).

Applications. Évaluation de la sécurité de RSA ; tables de nombres ; séquences aliquotes ; etc. Base pour les calculs de logarithme discret (ANR CATREL).

Partenaires. EPC CARAMEL (LORIA, P. Gaudry), 10+ développeurs; coding sprints, workshops, etc.

Utilisateurs. Cryptologique (RSA-768, RSA-704), factorisateurs au long cours (B_{400}), hackers (Z. Harris : clef trop courte dans Google, forge un email signé de Sergey Brin pour Larry Page).

Détails techniques. C/C++ basé sur GMP ; version pour calculs distribués (modèle client/serveur); LGPL 2.1 (ou supérieure); `http://cado-nfs.gforge.inria.fr`, version 2.0 (18/11/2013).

Performances. Sur un coeur de PC typique: 120 chiffres décimaux en 3 à 4 jours ; 140 en 1 mois ; 160 en 6 à 7 mois.

But ANR CADO. Fournir une implantation de référence complète de l'algorithme de factorisation d'entiers NFS (crible algébrique), qui permet de tester des idées nouvelles (sélection polynomiale).

Applications. Évaluation de la sécurité de RSA ; tables de nombres ; séquences aliquotes ; etc. Base pour les calculs de logarithme discret (ANR CATREL).

Partenaires. EPC CARAMEL (LORIA, P. Gaudry), 10+ développeurs; coding sprints, workshops, etc.

Utilisateurs. Cryptologique (RSA$_{768}$, RSA$_{704}$), factorisateurs au long cours (B_{400}), hackers (Z. Harris : clef trop courte dans Google, forge un email signé de Sergey Brin pour Larry Page).

Détails techniques. C/C++ basé sur GMP ; version pour calculs distribués (modèle client/serveur); LGPL 2.1 (ou supérieure); http://cado-nfs.gforge.inria.fr, version 2.0 (18/11/2013).

Performances. Sur un coeur de PC typique: 120 chiffres décimaux en 3 à 4 jours ; 140 en 1 mois ; 160 en 6 à 7 mois.

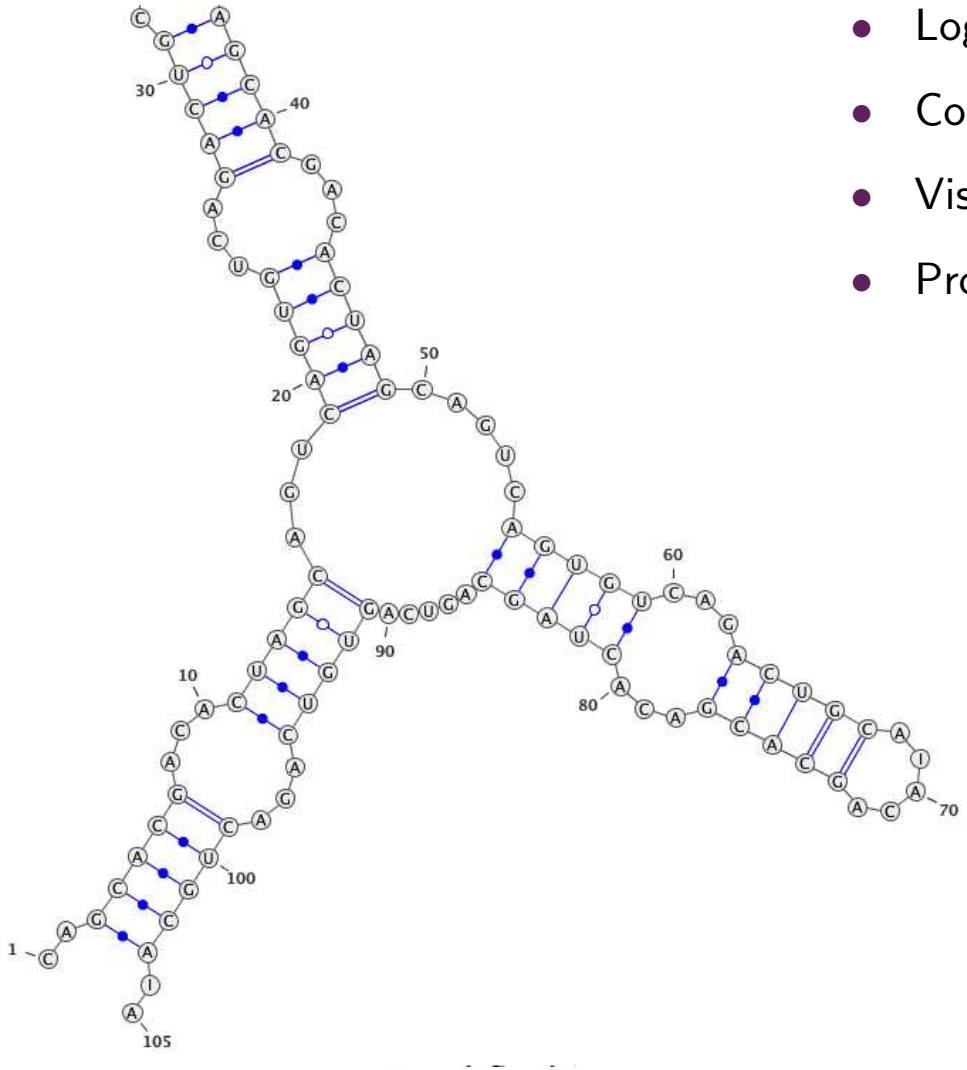
But. Un système de preuve automatique.

Auteurs. Commencé par A. Gacek (PhD Univ. of Minnesota, PostDoc LIX), et développements en cours au LIX.

Spécificités. Différent d'autres systèmes (comme Coq) : basé sur des relations (au lieu de fonctions), et permettant l'utilisation de λ-termes pour le syntaxe.

Points forts. Traitement immédiat et naturel de liaisons et de raisonnements inductifs et co-inductifs.

Applications. Le défi POPLMark et la meta-théorie du λ-calcul et du π-calcul.



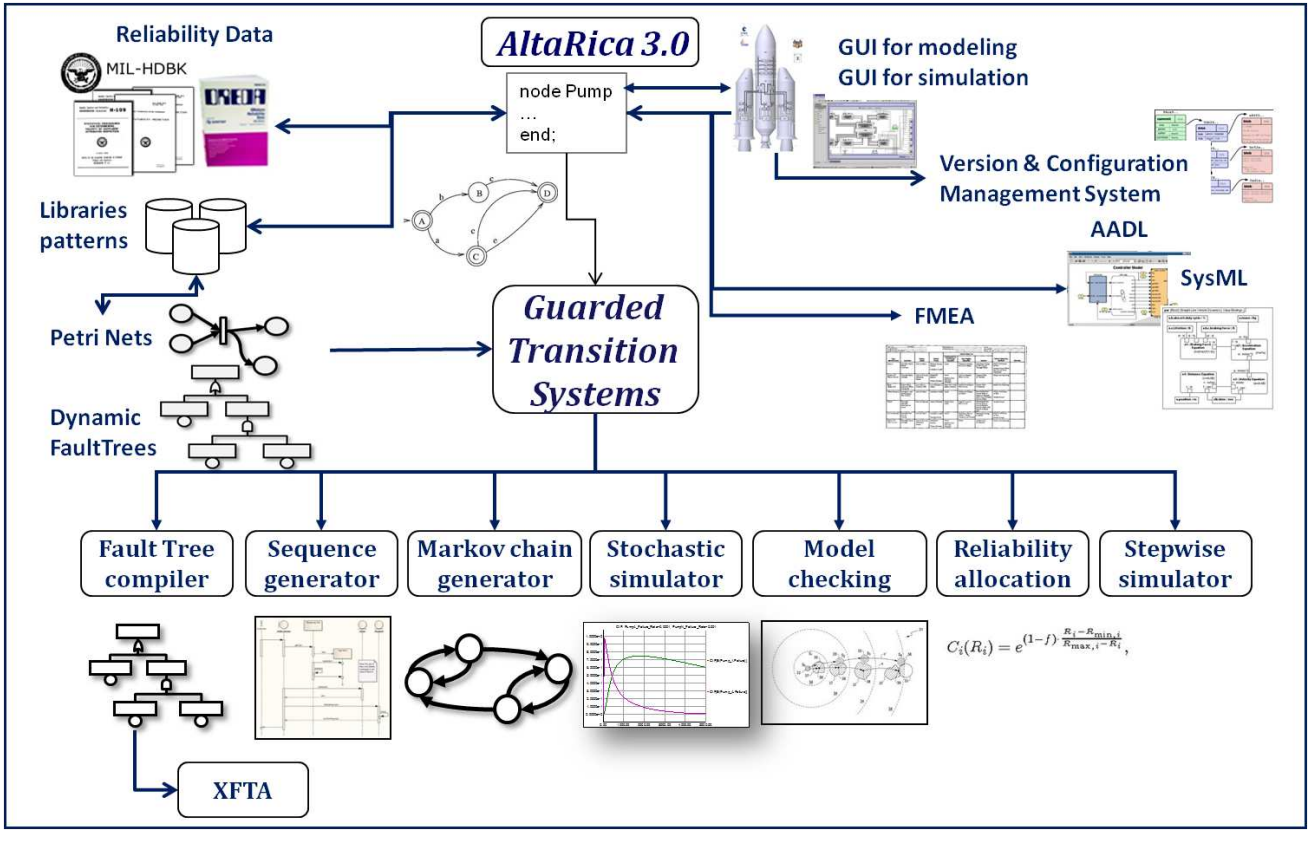
- Logiciel de visualisation de structures ARN
- Composant webservers/applications
- Visualisation interactive
- Production d'illustrations

⇝ Plus de détails sur poster

Description. AltaRica est un langage pour analyser la sécurité de systèmes industriels. Project Altarica 3.0 : nouvelle version du langage + série d'outils.

Applications. Centrales nucléaires (Areva/EDF) ou chimiques, avions (Dassault), etc.

Standardisation. Open-PSA → Modèles plus transparants et de meilleure qualité. Exemple : compatibilité entre EDF et Areva pour les centrales nucléaires.



Description. XFTA est un système complet pour calculer des arbres de défaillance.

Applications. Méthode probabiliste populaire pour évaluer les risques de sécurité pour des systèmes industriels comme les centrales nucléaires ou chimiques, les avions, etc.

Auteur. Antoine Rauzy.

Licence. Gratuit d'usage et de redistribution : `www.lix.polytechnique.fr/~rauzy`

Fonctionnalités.

- Intègre le format d'échange de modèles Open-PSA.
- Calcul d'ensembles minimaux de coupure ;
  implantation le plus efficace à l'heure actuelle.
- Calcul d'indicateurs de fiabilité pertinents : événements les plus probables, mesures d'importance, niveau de sécurité intégrée, etc.
- Analyse de sensitivité, dépendence par rapport au temps, etc.

Taille. $\approx$ 20.000 lignes de code C++

Perspectives. Intégration dans différents outils libres et industriels.

Mathemagix. Nouveau système de calcul formel et analytique libre

- Algorithmes reflétant meilleurs complexités théoriques, librairies actuellement en C++.
- Développement d'un nouveau langage haut niveau compilé et très efficace.
- Calcul mathématiquement exact avec objets de nature analytique.
- Collaboration avec l'équipe Galaad de Bernard MOURRAIN a Sophia.
- Environ 10 développeurs régulieurs + 30 plus occasionnels.

GNU TEXMACS. Suite bureautique scientifique libre

- Traitement de texte mathématique structuré, wysiwyg, facile d'utilisation.
- Alternative plus conviviale pour TEX/LATEX (et *pas* basé sur ces logiciels).
- Interface pour des systèmes de calcul formel, dont Mathemagix.
- Outil de présentation, dessins graphiques, tableur, contrôle des versions, etc.
- Édition de documents avec une sémantique riche.
- Pour Windows, MacOS et dans la plupart des distributions GNU/Linux.
- Entre 1000 et 10000 utilisateurs régulieurs.
- Environ 10 développeurs réguliers + 30 plus occasionnels.

Traitement de texte scientifique

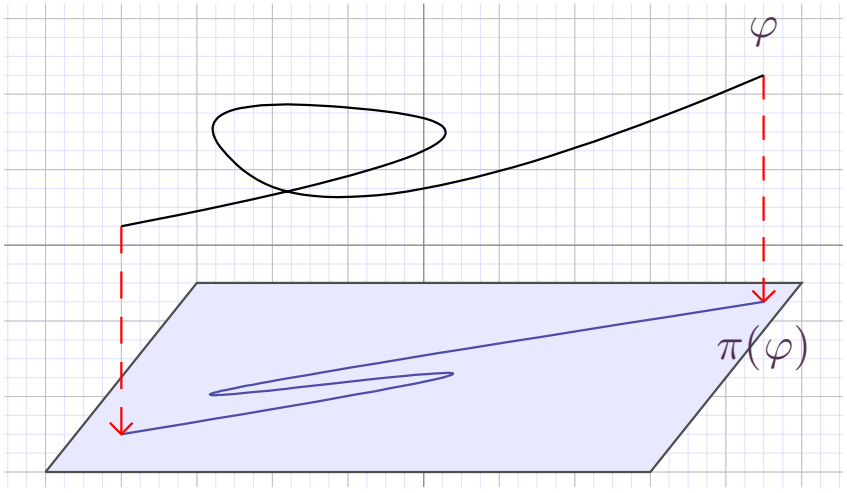
在这个环境中可以方便地输入多行公式，比如:

$$\begin{aligned} x+0 &= x \\ x+(-x) &= 0 \\ x+y &= y+x \\ (x+y)+z &= x+(y+z) \end{aligned}$$

第一列右对齐，第二列居中，第三列左对齐。

LaTeX source $\rightsquigarrow$ TEXMACS import

Graphiques



Tableur

$f(x)$	$\int f(x)\,\mathrm{d}x$ (par Maxima)
x^{2014}	=integrate(a2,x)
$\sin(x)\,x^2$	=integrate(a3,x)
$\frac{x^2}{x^2-x+2}$	=integrate(a4,x)

Présentations

Théorème 1

$e^{\pi i}+1=0$.

- Premier point.

Traitement de texte scientifique

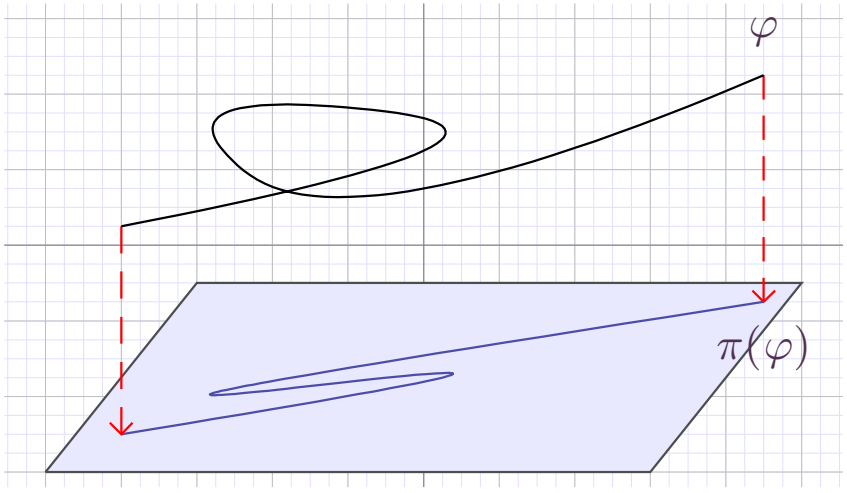
在这个环境中可以方便地输入多行公式，比如:

$$\begin{aligned} x+0 &= x \\ x+(-x) &= 0 \\ x+y &= y+x \\ (x+y)+z &= x+(y+z) \end{aligned}$$

第一列右对齐，第二列居中，第三列左对齐。

LaTeX source $\rightsquigarrow$ TEXMACS import

Graphiques



Tableur

$f(x)$	$\int f(x)\,\mathrm{d}x$ (par Maxima)
x^{2014}	$\frac{x^{2015}}{2015}$
$\sin(x)\,x^2$	=integrate(a3,x)
$\frac{x^2}{x^2-x+2}$	=integrate(a4,x)

Présentations

Théorème 2

$e^{\pi i}+1=0$.

- Premier point.

Traitement de texte scientifique

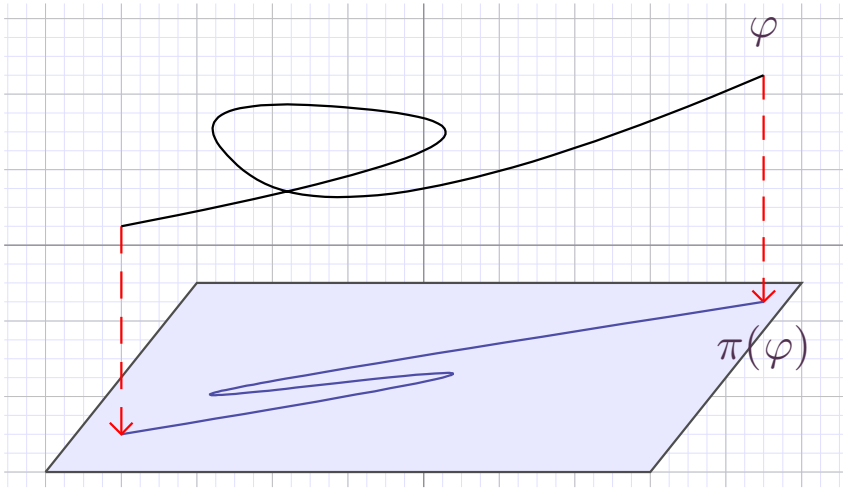
在这个环境中可以方便地输入多行公式，比如:

$$\begin{aligned} x+0 &= x \\ x+(-x) &= 0 \\ x+y &= y+x \\ (x+y)+z &= x+(y+z) \end{aligned}$$

第一列右对齐，第二列居中，第三列左对齐。

LaTeX source $\rightsquigarrow$ TEXMACS import

Graphiques



Tableur

$f(x)$	$\int f(x)\,\mathrm{d}x$ (par Maxima)
x^{2014}	$\frac{x^{2015}}{2015}$
$\sin(x)\,x^2$	$2\,x\sin(x)+(2-x^2)\cos(x)$
$\frac{x^2}{x^2-x+2}$	=integrate(a4,x)

Présentations

Théorème 3

$e^{\pi \mathrm{i}}+1=0$.

- Premier point.

Traitement de texte scientifique

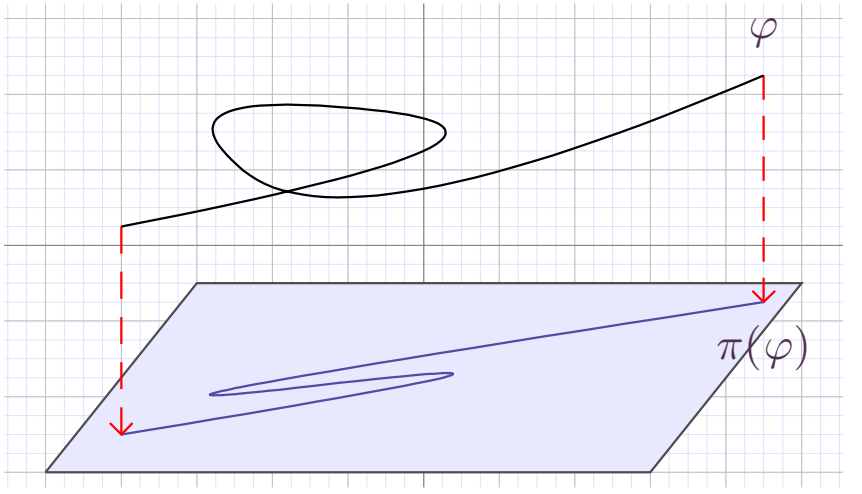
在这个环境中可以方便地输入多行公式， 比如:

$$\begin{aligned} x+0 &= x \\ x+(-x) &= 0 \\ x+y &= y+x \\ (x+y)+z &= x+(y+z) \end{aligned}$$

第一列右对齐， 第二列居中， 第三列左对齐。

LaTeX source $\rightsquigarrow$ TEXMACS import

Graphiques



Tableur

$f(x)$	$\int f(x)\,\mathrm{d}x$ (par Maxima)
x^{2014}	$\frac{x^{2015}}{2015}$
$\sin(x)\,x^2$	$2\,x\sin(x)+(2-x^2)\cos(x)$
$\frac{x^2}{x^2-x+2}$	$\frac{\log(x^2-x+2)}{2}-\frac{3\arctan\left(\frac{2x-1}{\sqrt{7}}\right)}{\sqrt{7}}+x$

Présentations

Théorème 4

$e^{\pi i}+1=0.$

- Premier point.

Traitement de texte scientifique

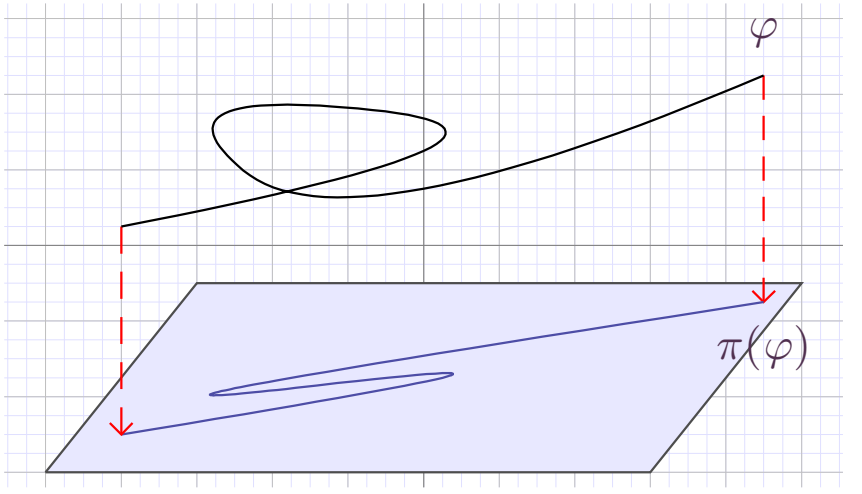
在这个环境中可以方便地输入多行公式， 比如:

$$\begin{aligned} x+0 &= x \\ x+(-x) &= 0 \\ x+y &= y+x \\ (x+y)+z &= x+(y+z) \end{aligned}$$

第一列右对齐， 第二列居中， 第三列左对齐。

LaTeX source $\rightsquigarrow$ TEXMACS import

Graphiques



Tableur

$f(x)$	$\int f(x)\,\mathrm{d}x$ (par Maxima)
x^{2014}	$\frac{x^{2015}}{2015}$
$\sin(x)\,x^2$	$2\,x\sin(x)+(2-x^2)\cos(x)$
$\frac{x^2}{x^2-x+2}$	$\frac{\log(x^2-x+2)}{2}-\frac{3\arctan\left(\frac{2x-1}{\sqrt{7}}\right)}{\sqrt{7}}+x$

Présentations

Théorème 5

$e^{\pi i}+1=0.$

- Premier point.
- Deuxième point.

Traitement de texte scientifique

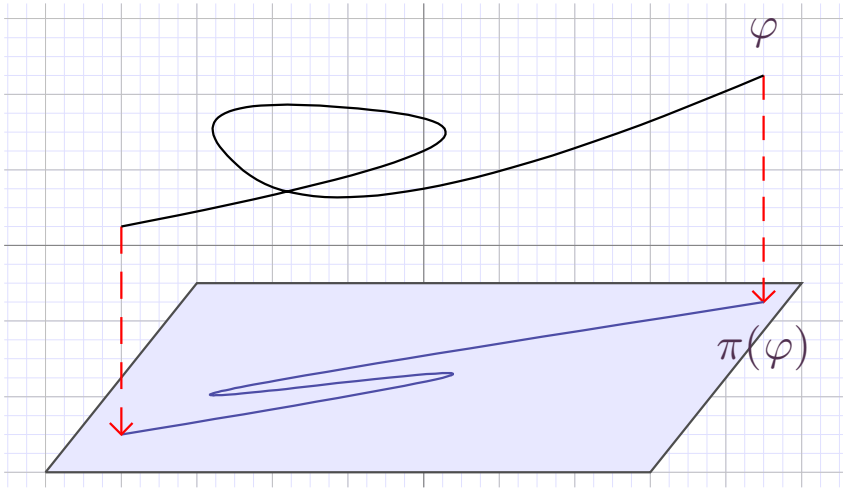
在这个环境中可以方便地输入多行公式， 比如:

$$\begin{aligned} x+0 &= x \\ x+(-x) &= 0 \\ x+y &= y+x \\ (x+y)+z &= x+(y+z) \end{aligned}$$

第一列右对齐， 第二列居中， 第三列左对齐。

LaTeX source $\rightsquigarrow$ TEXMACS import

Graphiques



Tableur

$f(x)$	$\int f(x)\,\mathrm{d}x$ (par Maxima)
x^{2014}	$\frac{x^{2015}}{2015}$
$\sin(x)\,x^2$	$2\,x\sin(x)+(2-x^2)\cos(x)$
$\frac{x^2}{x^2-x+2}$	$\frac{\log(x^2-x+2)}{2}-\frac{3\arctan\left(\frac{2x-1}{\sqrt{7}}\right)}{\sqrt{7}}+x$

Présentations

Théorème 6

$e^{\pi i}+1=0.$

- Premier point.
- Deuxième point.
- Formule animée :

⇑ Combinatoire / Calcul exact

```
Mmx] use "algebramix"
Mmx] z == series (0, 1);
Mmx] Bell == exp (exp z - 1)
Mmx] Bell[400] * 400!
Mmx]
```

⇑ Combinatoire / Calcul exact

```
Mmx] use "algebramix"
Mmx] z == series (0, 1);
Mmx] Bell == exp (exp z - 1)
```

$$1 + z + z^2 + \frac{5}{6} z^3 + \frac{5}{8} z^4 + \frac{13}{30} z^5 + \frac{203}{720} z^6 + \frac{877}{5040} z^7 + \frac{23}{224} z^8 + \frac{1007}{17280} z^9 + O(z^{10})$$

```
Mmx] Bell[400] * 400!
Mmx]
```

⇑ Combinatoire / Calcul exact

```
Mmx] use "algebramix"
```

```
Mmx] z == series (0, 1);
```

```
Mmx] Bell == exp (exp z - 1)
```

$$1 + z + z^2 + \frac{5}{6}z^3 + \frac{5}{8}z^4 + \frac{13}{30}z^5 + \frac{203}{720}z^6 + \frac{877}{5040}z^7 + \frac{23}{224}z^8 + \frac{1007}{17280}z^9 + O(z^{10})$$

```
Mmx] Bell[400] * 400!
```

```
128261995246769380878849989673162844495741812427678270882963180636242713855726064750\
041493604790719615032202203744120840979829987541290719640810163421805944472952349573\
078490531361422621871980416977066182696751060320587665082190181910410252271544052390\
717974326472656790314025578873635568845645400584805973271097847042478196686453300787\
300891763773694865852006882593762762263260471441616640746061449624503411091767251412\
037093827291613736030154437821736504863865642935807453979327881745329893681648026435\
116839710497456441373535396577921371775778857359061404334885411862355600684059066741\
083488562520584152801075233592774437164057586982965\
```

```
Mmx]
```

⇑ Combinatoire / Calcul numérique certifié

```
Mmx] use "analyziz"
Mmx] z == series (ball 0.0, ball 1.0);
Mmx] Bell == exp (exp z - 1)
Mmx] Bell[5000] * 5000!
Mmx]
```

⇑ Combinatoire / Calcul numérique certifié

```
Mmx] use "analyziz"
Mmx] z == series (ball 0.0, ball 1.0);
Mmx] Bell == exp (exp z - 1)
```

$$1.000000000000000000 + 1.000000000000000000\ z + 1.000000000000000000\ z^2 + 0.833333333333\backslash 3333\ z^3 + 0.625000000000000\ z^4 + 0.433333333333333\ z^5 + 0.2819444444444444\ z^6 + 0.17400793\backslash 650793651\ z^7 + 0.10267857142857143\ z^8 + 0.05827546296296296\ z^9 + O(z^{10})$$

```
Mmx] Bell[5000] * 5000!
Mmx]
```

⇑ Combinatoire / Calcul numérique certifié

```
Mmx] use "analyziz"
```

```
Mmx] z == series (ball 0.0, ball 1.0);
```

```
Mmx] Bell == exp (exp z - 1)
```

$$1.000000000000000000 + 1.000000000000000000\ z + 1.000000000000000000\ z^2 + 0.833333333333\backslash 3333\ z^3 + 0.625000000000000000\ z^4 + 0.433333333333333\ z^5 + 0.2819444444444444\ z^6 + 0.17400793\backslash 650793651\ z^7 + 0.10267857142857143\ z^8 + 0.05827546296296296\ z^9 + O(z^{10})$$

```
Mmx] Bell[5000] * 5000!
```

$$7.98038229677e12543$$

```
Mmx]
```

⇑ Résolution de systèmes polynomiaux

```
Mmx] use "geomsolvex"
Mmx] x == polynomial_dag (1 :> Rational, coordinate ('x));
Mmx] y == polynomial_dag (1 :> Rational, coordinate ('y));
Mmx] f1 == x^2 + y^2 - 1
Mmx] f2 == x^2 + x * y - 2
Mmx] geometric_solve_reduced_regular% ([f1, f2])
Mmx]
```

⇓

⇑ Résolution de systèmes polynomiaux

```
Mmx] use "geomsolvex"
Mmx] x == polynomial_dag (1 :> Rational, coordinate ('x));
Mmx] y == polynomial_dag (1 :> Rational, coordinate ('y));
Mmx] f1 == x^2 + y^2 - 1
```

$x^2 + y^2 - 1$

```
Mmx] f2 == x^2 + x * y - 2
Mmx] geometric_solve_reduced_regular% ([f1, f2])
Mmx]
```

⇓

⇑ Résolution de systèmes polynomiaux

```
Mmx] use "geomsolvex"
Mmx] x == polynomial_dag (1 :> Rational, coordinate ('x));
Mmx] y == polynomial_dag (1 :> Rational, coordinate ('y));
Mmx] f1 == x^2 + y^2 - 1
```

$$x^2 + y^2 - 1$$

```
Mmx] f2 == x^2 + x * y - 2
```

$$x^2 + x\,y - 2$$

```
Mmx] geometric_solve_reduced_regular% ([f1, f2])
Mmx]
```

⇓

⇑ Résolution de systèmes polynomiaux

```
Mmx] use "geomsolvex"
```

```
Mmx] x == polynomial_dag (1 :> Rational, coordinate ('x));
```

```
Mmx] y == polynomial_dag (1 :> Rational, coordinate ('y));
```

```
Mmx] f1 == x^2 + y^2 - 1
```

$$x^2 + y^2 - 1$$

```
Mmx] f2 == x^2 + x * y - 2
```

$$x^2 + x\,y - 2$$

```
Mmx] geometric_solve_reduced_regular% ([f1, f2])
```

$$\text{lifting\_fiber}\left(x^2 + y^2 - 1, x^2 + x\,y - 2, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, [0, 0], [], x, x^4 - \frac{5}{2}\,x^2 + 2, 4\,x^3 - 5\,x, [5\,x^2 - 8, 3\,x^2 - 2]\right)$$

```
Mmx]
```

⇓

⇑ Résolution de systèmes polynomiaux

```
Mmx] use "geomsolvex"
Mmx] x == polynomial_dag (1 :> Rational, coordinate ('x));
Mmx] y == polynomial_dag (1 :> Rational, coordinate ('y));
Mmx] f1 == x^2 + y^2 - 1
```

$$x^2 + y^2 - 1$$

```
Mmx] f2 == x^2 + x * y - 2
```

$$x^2 + x\,y - 2$$

```
Mmx] geometric_solve_reduced_regular% ([f1, f2])
```

$$\text{lifting\_fiber}\left(x^2 + y^2 - 1, x^2 + x\,y - 2, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, [0, 0], [], x, x^4 - \frac{5}{2}\,x^2 + 2, 4\,x^3 - 5\,x, [5\,x^2 - 8, 3\,x^2 - 2]\right)$$

```
Mmx]
```

⇑

$$x = \frac{5\,t^2 - 8}{4\,t^3 - 5\,t}, \quad y = \frac{3\,t^2 - 2}{4\,t^3 - 5\,t}, \quad t^4 - \frac{5}{2}\,t^2 + 2$$