Identités cachées

Friedrich Wehrung

Université de Caen
LMNO, CNRS UMR 6139
Département de Mathématiques
14032 Caen cedex
E-mail: friedrich.wehrung01@unicaen.fr
URL: http://www.math.unicaen.fr/˜wehrung

Coutances, le 17 mars 2014

Identités remarquables

Identités remarquables de base:

Identités remarquables

Identités remarquables de base:

- $(a+b)^2 = a^2 + 2ab + b^2$

Identités remarquables

Identités remarquables de base:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$

Identités remarquables

Identités remarquables de base:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a+b)(a-b) = a^2 - b^2.$

Identités remarquables

Identités remarquables de base:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a+b)(a-b) = a^2 - b^2.$

Identité de Karatsuba (Exercice indispensable!):

Identités remarquables

Identités remarquables de base:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a+b)(a-b) = a^2 - b^2$.

Identité de Karatsuba (Exercice indispensable!): Résout un problème posé en 1952 par Andrey Nikolaevich Kolmogorov (25 Avril 1903–20 Octobre 1987).

Identités remarquables

Identités remarquables de base:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a+b)(a-b) = a^2 - b^2.$

Identité de Karatsuba (Exercice indispensable!): Résout un problème posé en 1952 par Andrey Nikolaevich Kolmogorov (25 Avril 1903–20 Octobre 1987).

$$(100a_1 + a_0)(100b_1 + b_0) =$$
$$10\,000 a_1 b_1 + 100\big((a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1\big) + a_0 b_0$$

Identités remarquables

Identités remarquables de base:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a+b)(a-b) = a^2 - b^2$.

Identité de Karatsuba (Exercice indispensable!): Résout un problème posé en 1952 par Andrey Nikolaevich Kolmogorov (25 Avril 1903–20 Octobre 1987).

$$(100a_1 + a_0)(100b_1 + b_0) =$$
$$10\,000a_1b_1 + 100\big((a_0+a_1)(b_0+b_1) - a_0b_0 - a_1b_1\big) + a_0b_0$$

Le “100” ci-dessus peut être remplacé par un “B” quelconque, typiquement une puissance de 10 (ou de 2).

Identités remarquables

Identités remarquables de base:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a+b)(a-b) = a^2 - b^2$.

Identité de Karatsuba (Exercice indispensable!): Résout un problème posé en 1952 par Andrey Nikolaevich Kolmogorov (25 Avril 1903–20 Octobre 1987).

$$(100a_1 + a_0)(100b_1 + b_0) =$$
$$10\,000a_1b_1 + 100\big((a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1\big) + a_0b_0$$

Le "100" ci-dessus peut être remplacé par un "B" quelconque, typiquement une puissance de 10 (ou de 2). Le "10 000" ci-dessus devient alors B^2.

Anatoly Alexeevich Karatsuba (1937–2008)

Exemple d'utilisation de l'identité de Karatsuba:

$$(100a_1 + a_0)(100b_1 + b_0) =$$
$$10\,000a_1b_1 + 100\big((a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1\big) + a_0b_0$$

Exemple d'utilisation de l'identité de Karatsuba:

$$(100a_1 + a_0)(100b_1 + b_0) =$$
$$10\,000a_1 b_1 + 100\big((a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1\big) + a_0 b_0$$

Exemple:

$$2014 \times 8848 =$$

Exemple d'utilisation de l'identité de Karatsuba:

$$(100a_1 + a_0)(100b_1 + b_0) =$$
$$10\,000 a_1 b_1 + 100\big((a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1\big) + a_0 b_0$$

Exemple:

$$2014 \times 8848 = (100 \times \underbrace{20}_{a_1} + \underbrace{14}_{a_0}) \times (100 \times \underbrace{88}_{b_1} + \underbrace{48}_{b_0})$$

Exemple d'utilisation de l'identité de Karatsuba:

$$(100a_1 + a_0)(100b_1 + b_0) =$$
$$10\,000a_1b_1 + 100\big((a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1\big) + a_0b_0$$

Exemple:

$$2014 \times 8848 = (100 \times \underbrace{20}_{a_1} + \underbrace{14}_{a_0}) \times (100 \times \underbrace{88}_{b_1} + \underbrace{48}_{b_0})$$
$$= 10\,000 \times (\underbrace{20}_{a_1} \times \underbrace{88}_{b_1}) +$$
$$100 \times \Big(((\underbrace{14 + 20}_{a_0+a_1}) \times (\underbrace{48 + 88}_{b_0+b_1}))$$
$$- \underbrace{14}_{a_0} \times \underbrace{48}_{b_0} - \underbrace{20}_{a_1} \times \underbrace{88}_{b_1}\Big) + \underbrace{14}_{a_0} \times \underbrace{48}_{b_0}$$

. . . suite et fin de l'exemple

$$= 10\,000 \times (20 \times 88) +$$

. . . suite et fin de l'exemple

$$= 10\,000 \times (20 \times 88) +$$
$$100 \times (34 \times 136 - 14 \times 48 - 20 \times 88) + 14 \times 48$$

…suite et fin de l'exemple

$$
\begin{aligned}
&= 10\,000 \times (20 \times 88) + \\
&\quad 100 \times (34 \times 136 - 14 \times 48 - 20 \times 88) + 14 \times 48 \\
&= 17\,819\,872
\end{aligned}
$$

... suite et fin de l'exemple

$$
\begin{aligned}
&= 10\,000 \times (20 \times 88) + \\
&\quad 100 \times (34 \times 136 - 14 \times 48 - 20 \times 88) + 14 \times 48 \\
&= 17\,819\,872
\end{aligned}
$$

Point remarquable: ne demande que 3 multiplications

...suite et fin de l'exemple

$$
\begin{aligned}
&= 10\,000 \times (20 \times 88) + \\
&\quad 100 \times (34 \times 136 - 14 \times 48 - 20 \times 88) + 14 \times 48 \\
&= 17\,819\,872
\end{aligned}
$$

Point remarquable: ne demande que 3 multiplications (20×88, 14×48, 34×136) au lieu des 4 usuelles

. . . suite et fin de l'exemple

$$
\begin{aligned}
&= 10\,000 \times (20 \times 88) + \\
&\quad 100 \times (34 \times 136 - 14 \times 48 - 20 \times 88) + 14 \times 48 \\
&= 17\,819\,872
\end{aligned}
$$

Point remarquable: ne demande que 3 multiplications (20×88, 14×48, 34×136) au lieu des 4 usuelles (20×88, 20×48, 14×88, 14×48).

. . . suite et fin de l'exemple

$$= 10\,000 \times (20 \times 88) + \\ 100 \times (34 \times 136 - 14 \times 48 - 20 \times 88) + 14 \times 48 \\ = 17\,819\,872$$

Point remarquable: ne demande que 3 multiplications (20×88, 14×48, 34×136) au lieu des 4 usuelles (20×88, 20×48, 14×88, 14×48).
En utilisant la méthode de "divide and conquer" ("diviser pour régner"), permet de multiplier de grands nombres beaucoup plus rapidement.

...suite et fin de l'exemple

$$= 10\,000 \times (20 \times 88) + 100 \times (34 \times 136 - 14 \times 48 - 20 \times 88) + 14 \times 48$$
$$= 17\,819\,872$$

Point remarquable: ne demande que 3 multiplications (20×88, 14×48, 34×136) au lieu des 4 usuelles (20×88, 20×48, 14×88, 14×48).
En utilisant la méthode de "divide and conquer" ("diviser pour régner"), permet de multiplier de grands nombres beaucoup plus rapidement. Par exemple, pour deux nombres de $2^{10} = 1024$ chiffres, $3^{10} = 59\,048$ multiplications (K.) au lieu de $2^{20} = 1\,048\,576$ multiplications (méthode classique).

Domaine de validité des identités remarquables

Retour aux identités remarquables:

Domaine de validité des identités remarquables

Retour aux identités remarquables:

- $(a+b)^2 = a^2 + 2ab + b^2$

Domaine de validité des identités remarquables

Retour aux identités remarquables:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$

Domaine de validité des identités remarquables

Retour aux identités remarquables:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a+b)(a-b) = a^2 - b^2$.

Domaine de validité des identités remarquables

Retour aux identités remarquables:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a+b)(a-b) = a^2 - b^2$.

Valides pour n'importe quels nombres réels a et b.

Domaine de validité des identités remarquables

Retour aux identités remarquables:

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a+b)(a-b) = a^2 - b^2$.

Valides pour n'importe quels nombres réels a et b.
Et pour des objets plus généraux?

Matrices

- Matrices 2×2: Tableaux de nombres, de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Matrices

- Matrices 2×2: Tableaux de nombres, de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- Addition définie par

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} =$$

Matrices

- Matrices 2×2: Tableaux de nombres, de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- Addition définie par

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}.$$

Matrices

- Matrices 2×2: Tableaux de nombres, de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- Addition définie par

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}.$$

- Multiplication définie par

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} =$$

Matrices

- Matrices 2×2: Tableaux de nombres, de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- Addition définie par

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix} .$$

- Multiplication définie par

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix} .$$

Le zéro et l'unité chez les matrices

- La matrice nulle est $\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Le zéro et l'unité chez les matrices

- La matrice nulle est $\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Le zéro et l'unité chez les matrices

- La matrice nulle est $\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- La matrice unité est $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Le zéro et l'unité chez les matrices

- La matrice nulle est $\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- La matrice unité est $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Que deviennent les identités remarquables pour les matrices?

Exemple:

Que deviennent les identités remarquables pour les matrices?

Exemple: $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

Que deviennent les identités remarquables pour les matrices?

Exemple: $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

$$(a+b)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};$$

Que deviennent les identités remarquables pour les matrices?

Exemple: $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

$(a+b)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $a^2 + 2ab + b^2 = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$.

Que deviennent les identités remarquables pour les matrices?

Exemple: $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

$(a+b)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $a^2 + 2ab + b^2 = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$.

Pour cet exemple, $(a+b)^2 \neq a^2 + 2ab + b^2$.

Que deviennent les identités remarquables pour les matrices?

Exemple: $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

$(a+b)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $a^2 + 2ab + b^2 = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$.

Pour cet exemple, $(a+b)^2 \neq a^2 + 2ab + b^2$. De même, $(a-b)^2 \neq a^2 - 2ab + b^2$ et $(a+b)(a-b) \neq a^2 - b^2$.

Quel est le problème?

- Calcul de $(a+b)^2$, avec a et b matrices quelconques:

Quel est le problème?

- Calcul de $(a+b)^2$, avec a et b matrices quelconques:

$$(a+b)^2 = (a+b)(a+b)$$

Quel est le problème?

- Calcul de $(a+b)^2$, avec a et b matrices quelconques:

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\end{aligned}$$

Quel est le problème?

- Calcul de $(a+b)^2$, avec a et b matrices quelconques:

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= a^2+\underline{ab+ba}+b^2\end{aligned}$$

Quel est le problème?

- Calcul de $(a+b)^2$, avec a et b matrices quelconques:

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= a^2+\underline{ab+ba}+b^2\\ &\text{(et non pas } a^2+\underline{2ab}+b^2)\,.\end{aligned}$$

Quel est le problème?

- Calcul de $(a+b)^2$, avec a et b matrices quelconques:

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= a^2+\underline{ab+ba}+b^2\\ &\text{(et non pas } a^2+\underline{2ab}+b^2\text{)}.\end{aligned}$$

- Le problème est donc: $ab \neq ba$.

Domaine de validité

- Ainsi, pour des matrices a et b, “ $(a+b)^2 = a^2 + 2ab + b^2$ ” est équivalent à “ $ab = ba$ ”.

Domaine de validité

- Ainsi, pour des matrices a et b, " $(a+b)^2 = a^2 + 2ab + b^2$ " est équivalent à " $ab = ba$ ".
- On montre de même que chacune des deux autres identités remarquables, $(a-b)^2 = a^2 - 2ab + b^2$ et $(a+b)(a-b) = a^2 - b^2$, est équivalente à $ab = ba$.

Domaine de validité

- Ainsi, pour des matrices a et b, " $(a+b)^2 = a^2 + 2ab + b^2$ " est équivalent à " $ab = ba$ ".
- On montre de même que chacune des deux autres identités remarquables, $(a-b)^2 = a^2 - 2ab + b^2$ et $(a+b)(a-b) = a^2 - b^2$, est équivalente à $ab = ba$.
- Pour $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ (exemple précédent), on obtient $ab = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $ba = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Domaine de validité

- Ainsi, pour des matrices a et b, " $(a+b)^2 = a^2 + 2ab + b^2$ " est équivalent à " $ab = ba$ ".
- On montre de même que chacune des deux autres identités remarquables, $(a-b)^2 = a^2 - 2ab + b^2$ et $(a+b)(a-b) = a^2 - b^2$, est équivalente à $ab = ba$.
- Pour $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ (exemple précédent), on obtient $ab = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $ba = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
- Le raisonnement ci-dessus est valable dans tout anneau.

Anneaux

Identités définissant les anneaux (unitaires):

Anneaux

Identités définissant les anneaux (unitaires):

$$(x+y)+z = x+(y+z) \qquad (\text{associativité de } +)\,;$$

Anneaux

Identités définissant les anneaux (unitaires):

$$(x+y)+z = x+(y+z) \qquad \text{(associativité de } +\text{)} ;$$

$$x+y = y+x \qquad \text{(commutativité de } +\text{)} ;$$

Anneaux

Identités définissant les anneaux (unitaires):

$$
\begin{aligned}
(x+y)+z &= x+(y+z) && \text{(associativité de } +\text{)}\,; \\
x+y &= y+x && \text{(commutativité de } +\text{)}\,; \\
x+0 &= 0+x = x && \text{(0 est neutre pour } +\text{)}\,;
\end{aligned}
$$

Anneaux

Identités définissant les anneaux (unitaires):

$$
\begin{aligned}
(x+y)+z &= x+(y+z) && (\text{associativité de } +)\,; \\
x+y &= y+x && (\text{commutativité de } +)\,; \\
x+0 &= 0+x = x && (0 \text{ est neutre pour } +)\,; \\
x+(-x) &= (-x)+x = 0 && (-x \text{ est l'opposé de } x)\,;
\end{aligned}
$$

Anneaux

Identités définissant les anneaux (unitaires):

$$
\begin{aligned}
(x+y)+z = x+(y+z) &\qquad \text{(associativité de } +\text{)}\,; \\
x+y = y+x &\qquad \text{(commutativité de } +\text{)}\,; \\
x+0 = 0+x = x &\qquad \text{(0 est neutre pour } +\text{)}\,; \\
x+(-x) = (-x)+x = 0 &\qquad (-x \text{ est l'opposé de } x)\,; \\
(x\cdot y)\cdot z = x\cdot(y\cdot z) &\qquad \text{(associativité de } \cdot\text{)}\,;
\end{aligned}
$$

Anneaux

Identités définissant les anneaux (unitaires):

$$\begin{aligned}
(x+y)+z &= x+(y+z) && \text{(associativité de } +\text{)} ;\\
x+y &= y+x && \text{(commutativité de } +\text{)} ;\\
x+0 = 0+x &= x && \text{(0 est neutre pour } +\text{)} ;\\
x+(-x) = (-x)+x &= 0 && (-x \text{ est l'opposé de } x) ;\\
(x\cdot y)\cdot z &= x\cdot(y\cdot z) && \text{(associativité de } \cdot\text{)} ;\\
x\cdot(y+z) &= (x\cdot y)+(x\cdot z) && \text{(distributivité à gauche)} ;
\end{aligned}$$

Anneaux

Identités définissant les anneaux (unitaires):

$$
\begin{array}{cl}
(x+y)+z = x+(y+z) & (\text{associativité de } +)\,; \\
x+y = y+x & (\text{commutativité de } +)\,; \\
x+0 = 0+x = x & (0 \text{ est neutre pour } +)\,; \\
x+(-x) = (-x)+x = 0 & (-x \text{ est l'opposé de } x)\,; \\
(x\cdot y)\cdot z = x\cdot(y\cdot z) & (\text{associativité de } \cdot)\,; \\
x\cdot(y+z) = (x\cdot y)+(x\cdot z) & (\text{distributivité à gauche})\,; \\
(x+y)\cdot z = (x\cdot z)+(y\cdot z) & (\text{distributivité à droite})\,;
\end{array}
$$

Anneaux

Identités définissant les anneaux (unitaires):

$$
\begin{aligned}
(x+y)+z = x+(y+z) &\qquad \text{(associativité de } +\text{)}\,; \\
x+y = y+x &\qquad \text{(commutativité de } +\text{)}\,; \\
x+0 = 0+x = x &\qquad \text{(0 est neutre pour } +\text{)}\,; \\
x+(-x) = (-x)+x = 0 &\qquad (-x \text{ est l'opposé de } x)\,; \\
(x\cdot y)\cdot z = x\cdot(y\cdot z) &\qquad \text{(associativité de } \cdot\text{)}\,; \\
x\cdot(y+z) = (x\cdot y)+(x\cdot z) &\qquad \text{(distributivité à gauche)}\,; \\
(x+y)\cdot z = (x\cdot z)+(y\cdot z) &\qquad \text{(distributivité à droite)}\,; \\
x\cdot 1 = 1\cdot x = x &\qquad \text{(1 est neutre pour } \cdot\text{)}\,.
\end{aligned}
$$

Anneaux

Identités définissant les anneaux (unitaires):

$$
\begin{aligned}
(x+y)+z &= x+(y+z) && \text{(associativité de } +\text{)}\,; \\
x+y &= y+x && \text{(commutativité de } +\text{)}\,; \\
x+0 &= 0+x = x && \text{(0 est neutre pour } +\text{)}\,; \\
x+(-x) &= (-x)+x = 0 && (-x \text{ est l'opposé de } x)\,; \\
(x\cdot y)\cdot z &= x\cdot(y\cdot z) && \text{(associativité de } \cdot\text{)}\,; \\
x\cdot(y+z) &= (x\cdot y)+(x\cdot z) && \text{(distributivité à gauche)}\,; \\
(x+y)\cdot z &= (x\cdot z)+(y\cdot z) && \text{(distributivité à droite)}\,; \\
x\cdot 1 &= 1\cdot x = x && \text{(1 est neutre pour } \cdot\text{)}\,.
\end{aligned}
$$

L'identité $x\cdot y = y\cdot x$ (commutativité de $\cdot$) définit les anneaux commutatifs.

Des identités pour l'anneau des matrices 2×2, non satisfaites par tous les anneaux:

- La plus simple:

Des identités pour l'anneau des matrices 2×2, non satisfaites par tous les anneaux:

- La plus simple:
  $(ab - ba)^2 c = c(ab - ba)^2$.

Des identités pour l'anneau des matrices 2×2, non satisfaites par tous les anneaux:

- La plus simple:
  $(ab - ba)^2 c = c(ab - ba)^2$.
- Celle de plus petit degré (Amitsur-Levitzki, 1950):

Des identités pour l'anneau des matrices 2×2, non satisfaites par tous les anneaux:

- La plus simple:
  $(ab - ba)^2 c = c(ab - ba)^2$.
- Celle de plus petit degré (Amitsur-Levitzki, 1950):

$$
\begin{aligned}
& abcd - bacd - abdc + badc - acbd + cabd \\
& + acdb - cadb + adbc - dabc - adcb + dacb \\
& + cdab - cdba - dcab + dcba - bdac + bdca \\
& + dbac - dbca + bcad - bcda - cbad + cbda \\
& = 0\,.
\end{aligned}
$$

Une identité pour l'anneau des matrices $n \times n$:

- Identité d'Amitsur-Levitzki pour les matrices $n \times n$:

$$\sum_{\sigma \in \mathfrak{S}_{2n}} \operatorname{sgn}(\sigma) a_{\sigma(1)} \cdots a_{\sigma(2n)} = 0\,,$$

Une identité pour l'anneau des matrices $n \times n$:

- Identité d'Amitsur-Levitzki pour les matrices $n \times n$:

$$\sum_{\sigma \in \mathfrak{S}_{2n}} \operatorname{sgn}(\sigma) a_{\sigma(1)} \cdots a_{\sigma(2n)} = 0\,,$$

(où $\operatorname{sgn}(\sigma)$ est la "signature" de la permutation σ),

Une identité pour l'anneau des matrices $n \times n$:

- Identité d'Amitsur-Levitzki pour les matrices $n \times n$:

$$\sum_{\sigma \in \mathfrak{S}_{2n}} \operatorname{sgn}(\sigma) a_{\sigma(1)} \cdots a_{\sigma(2n)} = 0\,,$$

(où $\operatorname{sgn}(\sigma)$ est la "signature" de la permutation σ), pour toutes matrices $a_1, \ldots, a_{2n}$ à coefficients réels.

Une identité pour l'anneau des matrices $n \times n$:

- Identité d'Amitsur-Levitzki pour les matrices $n \times n$:

$$\sum_{\sigma \in \mathfrak{S}_{2n}} \operatorname{sgn}(\sigma) a_{\sigma(1)} \cdots a_{\sigma(2n)} = 0\,,$$

  (où $\operatorname{sgn}(\sigma)$ est la "signature" de la permutation σ), pour toutes matrices $a_1, \ldots, a_{2n}$ à coefficients réels.

- Remarque: Si une identité est satisfaite par tous les anneaux de matrices (de dimension quelconque), alors elle est satisfaite par tous les anneaux.

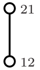
Une identité pour l'anneau des matrices $n \times n$:

- Identité d'Amitsur-Levitzki pour les matrices $n \times n$:

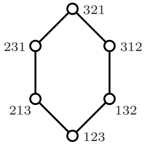
  $$\sum_{\sigma \in \mathfrak{S}_{2n}} \mathrm{sgn}(\sigma) a_{\sigma(1)} \cdots a_{\sigma(2n)} = 0\,,$$

  (où $\mathrm{sgn}(\sigma)$ est la "signature" de la permutation σ), pour toutes matrices $a_1, \ldots, a_{2n}$ à coefficients réels.
- Remarque: Si une identité est satisfaite par tous les anneaux de matrices (de dimension quelconque), alors elle est satisfaite par tous les anneaux. Peut être paraphrasé par "Il n'existe pas de version de l'identité d'Amitsur-Levitzki qui marche pour tous les n".

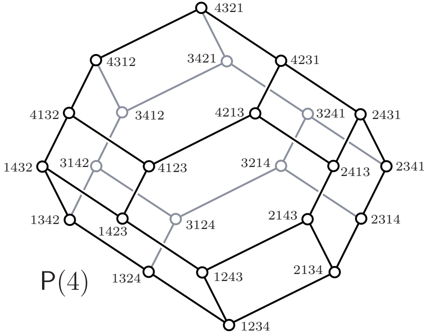
Treillis de permutations ("permutoèdres") sur 2, 3 et 4 lettres



P(2)



P(3)



P(4)

Si n est le "nombre d'inversions" de σ (hauteur de σ dans le permutoèdre), alors $\mathrm{sgn}(\sigma) = 1$ si n est pair, -1 sinon.

Anneaux booléens

- Les nombres entiers, réels, complexes forment des anneaux commutatifs.

Anneaux booléens

- Les nombres entiers, réels, complexes forment des anneaux commutatifs.
- Les matrices à coefficients réels forment un anneau, non commutatif.

Anneaux booléens

- Les nombres entiers, réels, complexes forment des anneaux commutatifs.
- Les matrices à coefficients réels forment un anneau, non commutatif.
- Le système d'identités [anneaux avec $x \cdot x = x$ (abrégé $x^2 = x$)] définit les

Anneaux booléens

- Les nombres entiers, réels, complexes forment des anneaux commutatifs.
- Les matrices à coefficients réels forment un anneau, non commutatif.
- Le système d'identités [anneaux avec $x \cdot x = x$ (abrégé $x^2 = x$)] définit les anneaux booléens

Anneaux booléens

- Les nombres entiers, réels, complexes forment des anneaux commutatifs.
- Les matrices à coefficients réels forment un anneau, non commutatif.
- Le système d'identités [anneaux avec $x \cdot x = x$ (abrégé $x^2 = x$)] définit les anneaux booléens (essentiels en logique et probabilités).

Anneaux booléens

- Les nombres entiers, réels, complexes forment des anneaux commutatifs.
- Les matrices à coefficients réels forment un anneau, non commutatif.
- Le système d'identités [anneaux avec $x \cdot x = x$ (abrégé $x^2 = x$)] définit les anneaux booléens (essentiels en logique et probabilités).
- Tout anneau booléen est commutatif.

Anneaux booléens

- Les nombres entiers, réels, complexes forment des anneaux commutatifs.
- Les matrices à coefficients réels forment un anneau, non commutatif.
- Le système d'identités [anneaux avec $x \cdot x = x$ (abrégé $x^2 = x$)] définit les anneaux booléens (essentiels en logique et probabilités).
- Tout anneau booléen est commutatif. *Preuve*:
  $x^2 = x \cdot x = x$, donc
  $4x = x^2 + x \cdot x + x \cdot x + x^2 = (x + x)^2 = x + x = 2x$ donne $2x = 0$; puis $x + y = (x + y)^2 = x + x \cdot y + y \cdot x + y$ donne $x \cdot y + y \cdot x = 0$; mais $x \cdot y + x \cdot y = 0$, d'où $x \cdot y = y \cdot x$).

Anneaux booléens

- Les nombres entiers, réels, complexes forment des anneaux commutatifs.
- Les matrices à coefficients réels forment un anneau, non commutatif.
- Le système d'identités [anneaux avec $x \cdot x = x$ (abrégé $x^2 = x$)] définit les anneaux booléens (essentiels en logique et probabilités).
- Tout anneau booléen est commutatif. *Preuve*: $x^2 = x \cdot x = x$, donc $4x = x^2 + x \cdot x + x \cdot x + x^2 = (x + x)^2 = x + x = 2x$ donne $2x = 0$; puis $x + y = (x + y)^2 = x + x \cdot y + y \cdot x + y$ donne $x \cdot y + y \cdot x = 0$; mais $x \cdot y + x \cdot y = 0$, d'où $x \cdot y = y \cdot x$).
- En fait, pour n'importe quel n, tout anneau satisfaisant l'identité $x^n = x$ est commutatif (difficile).

Anneaux booléens $\longrightarrow$ algèbres de Boole

- Dans un anneau booléen ($x^2 = x$), poser

Anneaux booléens $\longrightarrow$ algèbres de Boole

- Dans un anneau booléen ($x^2 = x$), poser $x \vee y = x + y + x \cdot y$, $x \wedge y = x \cdot y$, $\neg x = 1 + x$.

Anneaux booléens $\longrightarrow$ algèbres de Boole

- Dans un anneau booléen ($x^2 = x$), poser $x \vee y = x + y + x \cdot y$, $x \wedge y = x \cdot y$, $\neg x = 1 + x$.
- Algèbres de Boole:

Anneaux booléens $\longrightarrow$ algèbres de Boole

- Dans un anneau booléen ($x^2 = x$), poser $x \vee y = x + y + x \cdot y$, $x \wedge y = x \cdot y$, $\neg x = 1 + x$.
- Algèbres de Boole:

$$\text{(treillis)} \begin{cases} (x \vee y) \vee z = x \vee (y \vee z)\,; \\ x \vee y = y \vee x\,; \\ x \vee x = x\,; \\ (x \wedge y) \wedge z = x \wedge (y \wedge z)\,; \\ x \wedge y = y \wedge x\,; \\ x \wedge x = x\,; \\ x \wedge (x \vee y) = x \vee (x \wedge y) = x\,. \end{cases}$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)\,;$$

$$x \wedge \neg x = 0\,; x \vee \neg x = 1\,.$$

Algèbres de Boole $\leftrightarrow$ anneaux booléens

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.

Algèbres de Boole $\leftrightarrow$ anneaux booléens

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- Les transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ sont inverses l'une de l'autre.

Algèbres de Boole $\leftrightarrow$ anneaux booléens

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- Les transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ sont inverses l'une de l'autre.
- Les concepts d'algèbre de Boole et d'anneau booléen sont donc équivalents.

Algèbres de Boole $\leftrightarrow$ anneaux booléens

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- Les transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ sont inverses l'une de l'autre.
- Les concepts d'algèbre de Boole et d'anneau booléen sont donc équivalents.
- Exemple fondamental: on se fixe un ensemble E.

Algèbres de Boole $\leftrightarrow$ anneaux booléens

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- Les transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ sont inverses l'une de l'autre.
- Les concepts d'algèbre de Boole et d'anneau booléen sont donc équivalents.
- Exemple fondamental: on se fixe un ensemble E.
- L'ensemble de tous les sous-ensembles de E est une algèbre de Boole (resp., un anneau booléen), avec

Algèbres de Boole $\leftrightarrow$ anneaux booléens

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- Les transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ sont inverses l'une de l'autre.
- Les concepts d'algèbre de Boole et d'anneau booléen sont donc équivalents.
- Exemple fondamental: on se fixe un ensemble E.
- L'ensemble de tous les sous-ensembles de E est une algèbre de Boole (resp., un anneau booléen), avec
  - $0 = \varnothing$ (ensemble vide); $1 = E$ (ensemble "plein"); $X \vee Y = X \cup Y$ (réunion), $X \cdot Y = X \wedge Y = X \cap Y$ (intersection), $\neg X = E \setminus X$ (complémentaire);

Algèbres de Boole $\leftrightarrow$ anneaux booléens

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- Les transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ sont inverses l'une de l'autre.
- Les concepts d'algèbre de Boole et d'anneau booléen sont donc équivalents.
- Exemple fondamental: on se fixe un ensemble E.
- L'ensemble de tous les sous-ensembles de E est une algèbre de Boole (resp., un anneau booléen), avec
  - $0 = \varnothing$ (ensemble vide); $1 = E$ (ensemble "plein"); $X \vee Y = X \cup Y$ (réunion), $X \cdot Y = X \wedge Y = X \cap Y$ (intersection), $\neg X = E \setminus X$ (complémentaire);
  - $X + Y = (X \cup Y) \setminus (X \cap Y)$ (différence symétrique).

Algèbres de Robbins

- Identités:

$$(x \vee y) \vee z = x \vee (y \vee z)\,;$$

$$x \vee y = y \vee x\,;$$

$$\neg(\neg(x \vee y) + \neg(x \vee \neg y)) = x\,.$$

Algèbres de Robbins

- Identités:

$$
\begin{aligned}
(x \vee y) \vee z = x \vee (y \vee z)\,; \\
x \vee y = y \vee x\,; \\
\neg(\neg(x \vee y) + \neg(x \vee \neg y)) = x\,.
\end{aligned}
$$

- Toute algèbre de Boole est une algèbre de Robbins (exercice).

Algèbres de Robbins

- Identités:

$$\begin{aligned}(x \vee y) \vee z = x \vee (y \vee z)\,; \\ x \vee y = y \vee x\,; \\ \neg(\neg(x \vee y) + \neg(x \vee \neg y)) = x\,.\end{aligned}$$

- Toute algèbre de Boole est une algèbre de Robbins (exercice).
- Problème de la réciproque posé par Herbert Robbins en 1933.

Solution de la conjecture de Robbins

- Nombreuses tentatives infructueuses, par de nombreux mathématiciens dont Huntington, Robbins, Tarski.

Solution de la conjecture de Robbins

- Nombreuses tentatives infructueuses, par de nombreux mathématiciens dont Huntington, Robbins, Tarski.
- Problème finalement résolu en 1996 par William McCune (Décembre 1953–Mai 2011), qui a pour cela développé le logiciel de preuve automatique EQP.

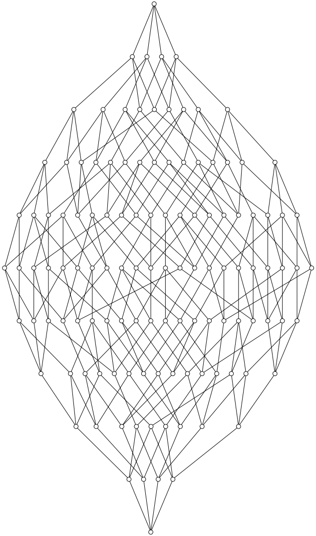
Solution de la conjecture de Robbins

- Nombreuses tentatives infructueuses, par de nombreux mathématiciens dont Huntington, Robbins, Tarski.
- Problème finalement résolu en 1996 par William McCune (Décembre 1953–Mai 2011), qui a pour cela développé le logiciel de preuve automatique EQP.
- McCune a ensuite développé EQP, qui est devenu le système de preuve / constructeur d'exemples Prover9-Mace4.

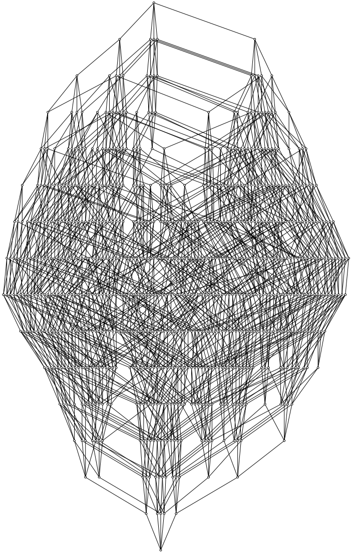
Solution de la conjecture de Robbins

- Nombreuses tentatives infructueuses, par de nombreux mathématiciens dont Huntington, Robbins, Tarski.
- Problème finalement résolu en 1996 par William McCune (Décembre 1953–Mai 2011), qui a pour cela développé le logiciel de preuve automatique EQP.
- McCune a ensuite développé EQP, qui est devenu le système de preuve / constructeur d'exemples Prover9-Mace4.

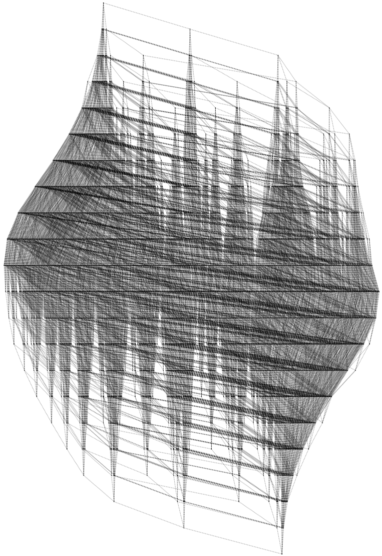
Le permutoèdre sur 5 lettres



Le permutoèdre sur 6 lettres



Le permutoèdre sur 7 lettres



Un mystère

- Tautologie: énoncé partout vrai (" $x * y = x * y$ ", " $x = y$ ou $x \neq y$ ", etc.)

Un mystère

- Tautologie: énoncé partout vrai (“ $x * y = x * y$ ”, “ $x = y$ ou $x \neq y$ ”, etc.)
- On pose $x * y = x^3 + y^2$, pour tous nombres entiers (ou réels, le problème est le même) x et y.

Un mystère

- Tautologie: énoncé partout vrai (“ $x * y = x * y$ ”, “ $x = y$ ou $x \neq y$ ”, etc.)
- On pose $x * y = x^3 + y^2$, pour tous nombres entiers (ou réels, le problème est le même) x et y.
- Existe-t-il une identité, non tautologique, satisfaite par cette opération $*$? (Problème posé sur la liste FOM il y a quelques années.)

Un mystère

- Tautologie: énoncé partout vrai (“ $x * y = x * y$ ”, “ $x = y$ ou $x \neq y$ ”, etc.)
- On pose $x * y = x^3 + y^2$, pour tous nombres entiers (ou réels, le problème est le même) x et y.
- Existe-t-il une identité, non tautologique, satisfaite par cette opération $*$? (Problème posé sur la liste FOM il y a quelques années.)
- Exemple de tentative: $x * y = x^3 + y^2$ n'est pas identique à $y * x = x^2 + y^3$. Donc l'identité $x * y = y * x$ n'est pas satisfaite.