Hidden identities

Friedrich Wehrung

Université de Caen
LMNO, CNRS UMR 6139
Département de Mathématiques
14032 Caen cedex
E-mail: friedrich.wehrung01@unicaen.fr
URL: http://wehrungf.users.lmno.cnrs.fr

December 22, 2017

“Remarkable identities”

Basic remarkable identities:

“Remarkable identities”

Basic remarkable identities:

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

"Remarkable identities"

Basic remarkable identities:

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

"Remarkable identities"

Basic remarkable identities:

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

“Remarkable identities”

Basic remarkable identities:

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

Karatsuba identity (To be checked as an exercise!):

"Remarkable identities"

Basic remarkable identities:

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

Karatsuba identity (To be checked as an exercise!): Solves a problem stated in 1952 by Andrey Nikolaevich Kolmogorov (April 25, 1903 – October 20, 1987).

"Remarkable identities"

Basic remarkable identities:

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

Karatsuba identity (To be checked as an exercise!): Solves a problem stated in 1952 by Andrey Nikolaevich Kolmogorov (April 25, 1903 – October 20, 1987).

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

"Remarkable identities"

Basic remarkable identities:

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

Karatsuba identity (To be checked as an exercise!): Solves a problem stated in 1952 by Andrey Nikolaevich Kolmogorov (April 25, 1903 – October 20, 1987).

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

The "100" above can be replaced by any B, typically a power of 10 (or of 2).

"Remarkable identities"

Basic remarkable identities:

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

Karatsuba identity (To be checked as an exercise!): Solves a problem stated in 1952 by Andrey Nikolaevich Kolmogorov (April 25, 1903 – October 20, 1987).

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

The "100" above can be replaced by any B, typically a power of 10 (or of 2). The "10,000" above then becomes B^2.

Anatoly Alexeevich Karatsuba (1937–2008)

Example of use of Karatsuba's identity:

$$(100a_1 + a_0)(100b_1 + b_0) =$$

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

Example of use of Karatsuba's identity:

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

Example:

$$2017 \times 8848 =$$

Example of use of Karatsuba's identity:

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

Example:

$$2017 \times 8848 = (100 \times \underbrace{20}_{a_1} + \underbrace{17}_{a_0}) \times (100 \times \underbrace{88}_{b_1} + \underbrace{48}_{b_0})$$

Example of use of Karatsuba's identity:

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

Example:

$$2017 \times 8848 = (100 \times \underbrace{20}_{a_1} + \underbrace{17}_{a_0}) \times (100 \times \underbrace{88}_{b_1} + \underbrace{48}_{b_0})$$
$$= 10{,}000 \times (\underbrace{20}_{a_1} \times \underbrace{88}_{b_1}) +$$
$$100 \times \Big(((\underbrace{17 + 20}_{a_0+a_1}) \times (\underbrace{48 + 88}_{b_0+b_1}))$$
$$- \underbrace{17}_{a_0} \times \underbrace{48}_{b_0} - \underbrace{20}_{a_1} \times \underbrace{88}_{b_1}\Big) + \underbrace{17}_{a_0} \times \underbrace{48}_{b_0}$$

...Example (cont'd)

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

. . . Example (cont'd)

$$= 10{,}000 \times (20 \times 88) +$$
$$100 \times (37 \times 136 - 17 \times 48 - 20 \times 88) + 17 \times 48$$

. . . Example (cont'd)

$$= 10{,}000 \times (20 \times 88) +$$
$$100 \times (37 \times 136 - 17 \times 48 - 20 \times 88) + 17 \times 48$$
$$= 17{,}846{,}416$$

... Example (cont'd)

$$= 10{,}000 \times (20 \times 88) + 100 \times (37 \times 136 - 17 \times 48 - 20 \times 88) + 17 \times 48$$
$$= 17{,}846{,}416$$

Remarkable point: this requires only 3 multiplications

. . . Example (cont'd)

$$= 10{,}000 \times (20 \times 88) + 100 \times (37 \times 136 - 17 \times 48 - 20 \times 88) + 17 \times 48$$
$$= 17{,}846{,}416$$

Remarkable point: this requires only 3 multiplications (i.e., 20×88, 17×48, 37×136) instead of the usual 4

. . . Example (cont'd)

$$= 10{,}000 \times (20 \times 88) + \\ 100 \times (37 \times 136 - 17 \times 48 - 20 \times 88) + 17 \times 48 \\ = 17{,}846{,}416$$

Remarkable point: this requires only 3 multiplications (i.e., 20×88, 17×48, 37×136) instead of the usual 4 (i.e., 20×88, 20×48, 17×88, 17×48).

... Example (cont'd)

$$= 10{,}000 \times (20 \times 88) + 100 \times (37 \times 136 - 17 \times 48 - 20 \times 88) + 17 \times 48$$
$$= 17{,}846{,}416$$

Remarkable point: this requires only 3 multiplications (i.e., 20×88, 17×48, 37×136) instead of the usual 4 (i.e., 20×88, 20×48, 17×88, 17×48).
By using the "divide and conquer" method, this enables to multiply large numbers much faster.

. . . Example (cont'd)

$$= 10{,}000 \times (20 \times 88) + 100 \times (37 \times 136 - 17 \times 48 - 20 \times 88) + 17 \times 48 = 17{,}846{,}416$$

Remarkable point: this requires only 3 multiplications (i.e., 20×88, 17×48, 37×136) instead of the usual 4 (i.e., 20×88, 20×48, 17×88, 17×48).
By using the "divide and conquer" method, this enables to multiply large numbers much faster. For example, with two numbers of $2^{10} = 1{,}024$ digits, $3^{10} = 59{,}048$ multiplications (Karatsuba multiplication) instead of $2^{20} = 1{,}048{,}576$ (classical multiplication).

... Example (cont'd)

$$= 10{,}000 \times (20 \times 88) + 100 \times (37 \times 136 - 17 \times 48 - 20 \times 88) + 17 \times 48 = 17{,}846{,}416$$

Remarkable point: this requires only 3 multiplications (i.e., 20×88, 17×48, 37×136) instead of the usual 4 (i.e., 20×88, 20×48, 17×88, 17×48).
By using the "divide and conquer" method, this enables to multiply large numbers much faster. For example, with two numbers of $2^{10} = 1{,}024$ digits, $3^{10} = 59{,}048$ multiplications (Karatsuba multiplication) instead of $2^{20} = 1{,}048{,}576$ (classical multiplication). There are even faster multiplication algorithms (e.g., FFT), but not so easy to implement.

Extending the validity range of remarkable identities

Hidden identities

Basic examples

Remarkable identities for matrices

Identities in rings

Other structures

Back to remarkable identities:

Extending the validity range of remarkable identities

Back to remarkable identities:

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

Extending the validity range of remarkable identities

Back to remarkable identities:

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

Extending the validity range of remarkable identities

Back to remarkable identities:

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

Extending the validity range of remarkable identities

Back to remarkable identities:

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

Valid for any real numbers a and b.

Extending the validity range of remarkable identities

Back to remarkable identities:

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

Valid for any real numbers a and b.
How about more general objects?

Matrices

- 2×2 matrices: Arrays of numbers of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Matrices

- 2×2 matrices: Arrays of numbers of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- Addition defined by

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

Matrices

- 2×2 matrices: Arrays of numbers of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- Addition defined by

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

Matrices

- 2×2 matrices: Arrays of numbers of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- Addition defined by

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

- Multiplication defined by

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

Matrices

- 2×2 matrices: Arrays of numbers of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- Addition defined by

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

- Multiplication defined by

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

The zero and the unit for matrices

- The zero matrix is $\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

The zero and the unit for matrices

- The zero matrix is $\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

The zero and the unit for matrices

- The zero matrix is $\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- The unit matrix is $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

The zero and the unit for matrices

- The zero matrix is $\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- The unit matrix is $\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Checking remarkable identities on matrices

Example:

Checking remarkable identities on matrices

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

Checking remarkable identities on matrices

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

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

Checking remarkable identities on matrices

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

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

Checking remarkable identities on matrices

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

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

For this example, $(a+b)^2 \neq a^2 + 2ab + b^2$.

Checking remarkable identities on matrices

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

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

For this example, $(a+b)^2 \neq a^2 + 2ab + b^2$. Similarly, $(a-b)^2 \neq a^2 - 2ab + b^2$ and $(a+b)(a-b) \neq a^2 - b^2$.

What's the problem?

- Computing $(a+b)^2$, for arbitrary matrices a and b:

What's the problem?

- Computing $(a+b)^2$, for arbitrary matrices a and b:

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

What's the problem?

- Computing $(a+b)^2$, for arbitrary matrices a and b:

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

What's the problem?

- Computing $(a+b)^2$, for arbitrary matrices a and b:

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

What's the problem?

- Computing $(a+b)^2$, for arbitrary matrices a and b:

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= a^2+\underline{ab+ba}+b^2\\ &\text{(as opposed to } a^2+\underline{2ab}+b^2\text{)}\,.\end{aligned}$$

What's the problem?

- Computing $(a+b)^2$, for arbitrary matrices a and b:

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= a^2+\underline{ab+ba}+b^2\\ &\text{(as opposed to } a^2+\underline{2ab}+b^2)\,.\end{aligned}$$

- Hence the problem boils down to $ab \neq ba$.

Validity range

- Hence, for matrices a and b, " $(a+b)^2 = a^2 + 2ab + b^2$ " is equivalent to " $ab = ba$ ".

Validity range

- Hence, for matrices a and b, " $(a+b)^2 = a^2 + 2ab + b^2$ " is equivalent to " $ab = ba$ ".
- Similarly, each of the other two remarkable identities, $(a-b)^2 = a^2 - 2ab + b^2$, and $(a+b)(a-b) = a^2 - b^2$, is also equivalent to $ab = ba$.

Validity range

- Hence, for matrices a and b, " $(a+b)^2 = a^2 + 2ab + b^2$ " is equivalent to " $ab = ba$ ".
- Similarly, each of the other two remarkable identities, $(a-b)^2 = a^2 - 2ab + b^2$, and $(a+b)(a-b) = a^2 - b^2$, is also equivalent to $ab = ba$.
- For $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ (previous example), we obtain $ab = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $ba = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Validity range

- Hence, for matrices a and b, " $(a+b)^2 = a^2 + 2ab + b^2$ " is equivalent to " $ab = ba$ ".
- Similarly, each of the other two remarkable identities, $(a-b)^2 = a^2 - 2ab + b^2$, and $(a+b)(a-b) = a^2 - b^2$, is also equivalent to $ab = ba$.
- For $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ (previous example), we obtain $ab = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $ba = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
- The argument above is valid in any ring.

Rings

Defining identities for (unital) rings:

Rings

Defining identities for (unital) rings:

$$(x + y) + z = x + (y + z) \qquad \text{(associativity of } +\text{)};$$

Rings

Defining identities for (unital) rings:

$$(x + y) + z = x + (y + z) \qquad \text{(associativity of } +\text{)};$$
$$x + y = y + x \qquad \text{(commutativity of } +\text{)};$$

Rings

Defining identities for (unital) rings:

$$
\begin{aligned}
(x+y)+z &= x+(y+z) && (\text{associativity of } +)\,;\\
x+y &= y+x && (\text{commutativity of } +)\,;\\
x+0 = 0+x &= x && (0 \text{ is neutral pour } +)\,;
\end{aligned}
$$

Rings

Defining identities for (unital) rings:

$(x + y) + z = x + (y + z)$	(associativity of $+$) ;
$x + y = y + x$	(commutativity of $+$) ;
$x + 0 = 0 + x = x$	(0 is neutral pour $+$) ;
$x + (-x) = (-x) + x = 0$	($-x$ is the opposite of x) ;

Rings

Defining identities for (unital) rings:

$$(x+y)+z = x+(y+z) \qquad \text{(associativity of } +\text{)};$$
$$x+y = y+x \qquad \text{(commutativity of } +\text{)};$$
$$x+0 = 0+x = x \qquad \text{(0 is neutral pour } +\text{)};$$
$$x+(-x) = (-x)+x = 0 \qquad (-x \text{ is the opposite of } x);$$
$$(x\cdot y)\cdot z = x\cdot(y\cdot z) \qquad \text{(associativity of } \cdot\text{)};$$

Rings

Defining identities for (unital) rings:

$$(x + y) + z = x + (y + z) \quad \text{(associativity of } +\text{)} ;$$

$$x + y = y + x \quad \text{(commutativity of } +\text{)} ;$$

$$x + 0 = 0 + x = x \quad \text{(0 is neutral pour } +\text{)} ;$$

$$x + (-x) = (-x) + x = 0 \quad (-x \text{ is the opposite of } x) ;$$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \text{(associativity of } \cdot\text{)} ;$$

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \quad \text{(left distributivity)} ;$$

Rings

Defining identities for (unital) rings:

$(x+y)+z = x+(y+z)$	(associativity of $+$) ;
$x+y = y+x$	(commutativity of $+$) ;
$x+0 = 0+x = x$	(0 is neutral pour $+$) ;
$x+(-x) = (-x)+x = 0$	($-x$ is the opposite of x) ;
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	(associativity of $\cdot$) ;
$x \cdot (y+z) = (x \cdot y) + (x \cdot z)$	(left distributivity) ;
$(x+y) \cdot z = (x \cdot z) + (y \cdot z)$	(right distributivity) ;

Rings

Defining identities for (unital) rings:

$$
\begin{aligned}
(x+y)+z &= x+(y+z) && \text{(associativity of } +\text{)}\,; \\
x+y &= y+x && \text{(commutativity of } +\text{)}\,; \\
x+0 &= 0+x = x && \text{(0 is neutral pour } +\text{)}\,; \\
x+(-x) &= (-x)+x = 0 && (-x \text{ is the opposite of } x)\,; \\
(x\cdot y)\cdot z &= x\cdot(y\cdot z) && \text{(associativity of } \cdot\text{)}\,; \\
x\cdot(y+z) &= (x\cdot y)+(x\cdot z) && \text{(left distributivity)}\,; \\
(x+y)\cdot z &= (x\cdot z)+(y\cdot z) && \text{(right distributivity)}\,; \\
x\cdot 1 &= 1\cdot x = x && \text{(1 is neutral for } \cdot\text{)}\,.
\end{aligned}
$$

Rings

Defining identities for (unital) rings:

$$\begin{aligned}
(x+y)+z = x+(y+z) &\quad \text{(associativity of } +\text{)} ; \\
x+y = y+x &\quad \text{(commutativity of } +\text{)} ; \\
x+0 = 0+x = x &\quad \text{(0 is neutral pour } +\text{)} ; \\
x+(-x) = (-x)+x = 0 &\quad \text{(} -x \text{ is the opposite of } x\text{)} ; \\
(x \cdot y) \cdot z = x \cdot (y \cdot z) &\quad \text{(associativity of } \cdot\text{)} ; \\
x \cdot (y+z) = (x \cdot y) + (x \cdot z) &\quad \text{(left distributivity)} ; \\
(x+y) \cdot z = (x \cdot z) + (y \cdot z) &\quad \text{(right distributivity)} ; \\
x \cdot 1 = 1 \cdot x = x &\quad \text{(1 is neutral for } \cdot\text{)} .
\end{aligned}$$

The identity $x \cdot y = y \cdot x$ (commutativity of $\cdot$) defines commutative rings.

Identities for rings of 2×2 matrices, not valid in all rings:

- The easiest:

Identities for rings of 2×2 matrices, not valid in all rings:

- The easiest:
  $(ab - ba)^2 c = c(ab - ba)^2$.

Identities for rings of 2×2 matrices, not valid in all rings:

- The easiest:
  $(ab - ba)^2 c = c(ab - ba)^2$.
- The one with smallest degree (Amitsur-Levitzki, 1950):

Identities for rings of 2×2 matrices, not valid in all rings:

- The easiest:
  $(ab - ba)^2 c = c(ab - ba)^2$.
- The one with smallest degree (Amitsur-Levitzki, 1950):

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

An identity for all $n \times n$ matrices:

- The Amitsur-Levitzki identity for $n \times n$ matrices:

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

An identity for all $n \times n$ matrices:

- The Amitsur-Levitzki identity for $n \times n$ matrices:

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

(here, $\operatorname{sgn}(\sigma)$ denotes the "signature" of the permutation σ),

An identity for all $n \times n$ matrices:

- The Amitsur-Levitzki identity for $n \times n$ matrices:

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

(here, $\operatorname{sgn}(\sigma)$ denotes the “signature” of the permutation σ), for all $n \times n$ real matrices $a_1, \ldots, a_{2n}$.

An identity for all $n \times n$ matrices:

- The Amitsur-Levitzki identity for $n \times n$ matrices:

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

(here, $\operatorname{sgn}(\sigma)$ denotes the "signature" of the permutation σ), for all $n \times n$ real matrices $a_1, \ldots, a_{2n}$.

- Remark: If an identity holds in all real matrix rings (of arbitrary dimension), then it holds in all rings.

An identity for all $n \times n$ matrices:

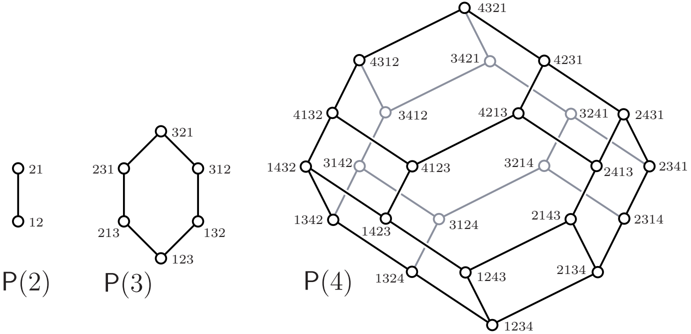
- The Amitsur-Levitzki identity for $n \times n$ matrices:

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

  (here, $\operatorname{sgn}(\sigma)$ denotes the "signature" of the permutation σ), for all $n \times n$ real matrices $a_1, \ldots, a_{2n}$.

- Remark: If an identity holds in all real matrix rings (of arbitrary dimension), then it holds in all rings. This implies that "there is no version of the Amitsur-Levitzki identity that holds for all n".

Permutation lattices (“permutohedra”) on 2, 3, and 4 letters



If n is the number of inversions of σ (height of σ in the permutohedron), then $\text{sgn}(\sigma) = 1$ if n is even, -1 if n is odd.

Boolean rings

- Integers, reals, complex numbers all form commutative rings.

Boolean rings

- Integers, reals, complex numbers all form commutative rings.
- 2×2 real matrices form a non commutative ring.

Boolean rings

- Integers, reals, complex numbers all form commutative rings.
- 2×2 real matrices form a non commutative ring.
- The system of identities [rings with $x \cdot x = x$ (abbreviated $x^2 = x$)] defines

Boolean rings

- Integers, reals, complex numbers all form commutative rings.
- 2×2 real matrices form a non commutative ring.
- The system of identities [rings with $x \cdot x = x$ (abbreviated $x^2 = x$)] defines Boolean rings

Boolean rings

- Integers, reals, complex numbers all form commutative rings.
- 2×2 real matrices form a non commutative ring.
- The system of identities [rings with $x \cdot x = x$ (abbreviated $x^2 = x$)] defines Boolean rings (important in logic and probability theory).

Boolean rings

- Integers, reals, complex numbers all form commutative rings.
- 2×2 real matrices form a non commutative ring.
- The system of identities [rings with $x \cdot x = x$ (abbreviated $x^2 = x$)] defines Boolean rings (important in logic and probability theory).
- Every Boolean ring is commutative.

Boolean rings

- Integers, reals, complex numbers all form commutative rings.
- 2×2 real matrices form a non commutative ring.
- The system of identities [rings with $x \cdot x = x$ (abbreviated $x^2 = x$)] defines Boolean rings (important in logic and probability theory).
- Every Boolean ring is commutative. (*Proof*: $x^2 = x \cdot x = x$, thus $4x = x^2 + x \cdot x + x \cdot x + x^2 = (x + x)^2 = x + x = 2x$, which yields $2x = 0$; then $x + y = (x + y)^2 = x + x \cdot y + y \cdot x + y$ yields $x \cdot y + y \cdot x = 0$; however, $x \cdot y + x \cdot y = 0$, thus $x \cdot y = y \cdot x$).

Boolean rings

- Integers, reals, complex numbers all form commutative rings.
- 2×2 real matrices form a non commutative ring.
- The system of identities [rings with $x \cdot x = x$ (abbreviated $x^2 = x$)] defines Boolean rings (important in logic and probability theory).
- Every Boolean ring is commutative. (*Proof*: $x^2 = x \cdot x = x$, thus $4x = x^2 + x \cdot x + x \cdot x + x^2 = (x + x)^2 = x + x = 2x$, which yields $2x = 0$; then $x + y = (x + y)^2 = x + x \cdot y + y \cdot x + y$ yields $x \cdot y + y \cdot x = 0$; however, $x \cdot y + x \cdot y = 0$, thus $x \cdot y = y \cdot x$).
- In fact, for every positive integer n, every ring satisfying the identity $x^n = x$ is commutative (difficult result!).

Boolean rings → Boolean algebras

- In any Boolean ring ($x^2 = x$), set

Boolean rings → Boolean algebras

- In any Boolean ring ($x^2 = x$), set
  $x \vee y = x + y + x \cdot y$, $x \wedge y = x \cdot y$, $\neg x = 1 + x$.

Boolean rings → Boolean algebras

- In any Boolean ring ($x^2 = x$), set $x \vee y = x + y + x \cdot y$, $x \wedge y = x \cdot y$, $\neg x = 1 + x$.
- Boolean algebras:

Boolean rings → Boolean algebras

- In any Boolean ring ($x^2 = x$), set
  $x \vee y = x + y + x \cdot y$, $x \wedge y = x \cdot y$, $\neg x = 1 + x$.
- Boolean algebras:

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

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

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

Boolean algebras $\leftrightarrow$ Boolean rings

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

Boolean algebras $\leftrightarrow$ Boolean rings

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- The transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ are mutually inverse.

Boolean algebras $\leftrightarrow$ Boolean rings

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- The transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ are mutually inverse.
- The concepts of Boolean algebra and Boolean ring are thus equivalent.

Boolean algebras $\leftrightarrow$ Boolean rings

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- The transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ are mutually inverse.
- The concepts of Boolean algebra and Boolean ring are thus equivalent.
- Fundamental example: let us fix a set E.

Boolean algebras $\leftrightarrow$ Boolean rings

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- The transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ are mutually inverse.
- The concepts of Boolean algebra and Boolean ring are thus equivalent.
- Fundamental example: let us fix a set E.
- The set of all subsets of E is a Boolean algebra (resp., a Boolean ring), with

Boolean algebras $\leftrightarrow$ Boolean rings

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- The transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ are mutually inverse.
- The concepts of Boolean algebra and Boolean ring are thus equivalent.
- Fundamental example: let us fix a set E.
- The set of all subsets of E is a Boolean algebra (resp., a Boolean ring), with
  - $0 = \varnothing$ (empty set); $1 = E$ ("full" set); $X \vee Y = X \cup Y$ (union), $X \cdot Y = X \wedge Y = X \cap Y$ (intersection), $\neg X = E \setminus X$ (complement);

Boolean algebras $\leftrightarrow$ Boolean rings

- $x + y = (x \vee y) \wedge \neg(x \wedge y)$, $x \cdot y = x \wedge y$.
- The transformations $(0, 1, +, \cdot) \leftrightharpoons (0, 1, \vee, \wedge, \neg)$ are mutually inverse.
- The concepts of Boolean algebra and Boolean ring are thus equivalent.
- Fundamental example: let us fix a set E.
- The set of all subsets of E is a Boolean algebra (resp., a Boolean ring), with
  - $0 = \varnothing$ (empty set); $1 = E$ ("full" set); $X \vee Y = X \cup Y$ (union), $X \cdot Y = X \wedge Y = X \cap Y$ (intersection), $\neg X = E \setminus X$ (complement);
  - $X + Y = (X \cup Y) \setminus (X \cap Y)$ (symmetric difference).

Robbins algebras

- Identities:

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

Robbins algebras

- Identities:

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

- Every Boolean algebra is a Robbins algebra (exercise).

Robbins algebras

- Identities:

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

- Every Boolean algebra is a Robbins algebra (exercise).
- The problem of the converse was stated by Herbert Robbins in 1933.

Solution of the Robbins conjecture

- There were many unsuccessful attempts from a number of mathematicians, including Huntington, Robbins, Tarski.

Solution of the Robbins conjecture

- There were many unsuccessful attempts from a number of mathematicians, including Huntington, Robbins, Tarski.
- The problem was finally solved (positively) in 1996 by William McCune (December 1953 – May 2011), who created for that purpose the software EQP.

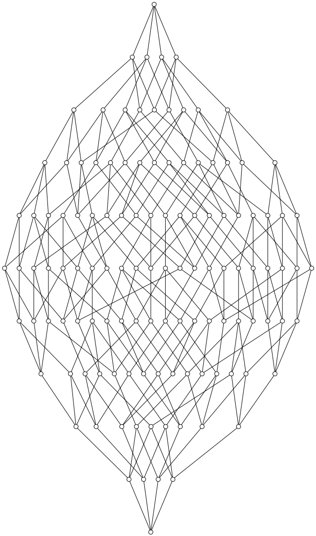
Solution of the Robbins conjecture

- There were many unsuccessful attempts from a number of mathematicians, including Huntington, Robbins, Tarski.
- The problem was finally solved (positively) in 1996 by William McCune (December 1953 – May 2011), who created for that purpose the software EQP.
- Further building on EQP, McCune developed the automatic prover / counterexample builder Prover9-Mace4 (see `http://www.cs.unm.edu/~mccune/mace4/`).

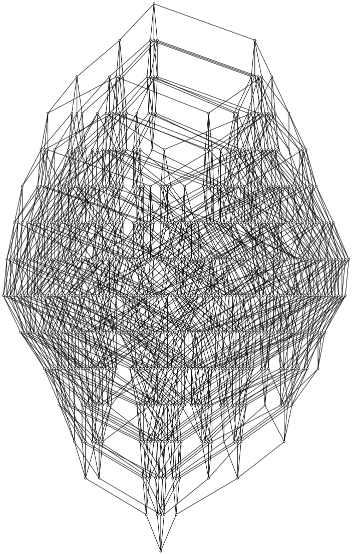
Solution of the Robbins conjecture

- There were many unsuccessful attempts from a number of mathematicians, including Huntington, Robbins, Tarski.
- The problem was finally solved (positively) in 1996 by William McCune (December 1953 – May 2011), who created for that purpose the software EQP.
- Further building on EQP, McCune developed the automatic prover / counterexample builder Prover9-Mace4 (see `http://www.cs.unm.edu/~mccune/mace4/`).

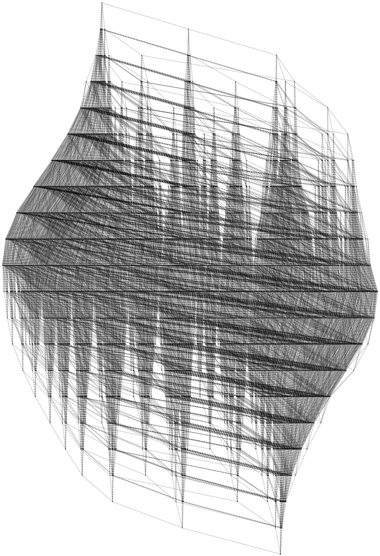
The permutohedron on 5 letters



The permutohedron on 6 letters



The permutohedron on 7 letters



Theorem (Santocanale and W. 2014)

There exists an identity, on the operations $\vee$ (join) and $\wedge$ (meet), that holds in all permutohedra $\mathrm{P}(n)$ (i.e., in all permutation lattices), but that does not hold in all (finite) lattices.

- This identity does not hold in all lattices $(L, \vee, \wedge)$:

Theorem (Santocanale and W. 2014)

There exists an identity, on the operations $\vee$ (join) and $\wedge$ (meet), that holds in all permutohedra $\mathrm{P}(n)$ (i.e., in all permutation lattices), but that does not hold in all (finite) lattices.

- This identity does not hold in all lattices $(L, \vee, \wedge)$: in fact, it holds in all lattices with up to 3,337 elements, and it fails in a 3,338-element lattice.

Theorem (Santocanale and W. 2014)

There exists an identity, on the operations $\vee$ (join) and $\wedge$ (meet), that holds in all permutohedra $\mathrm{P}(n)$ (i.e., in all permutation lattices), but that does not hold in all (finite) lattices.

- This identity does not hold in all lattices $(L, \vee, \wedge)$: in fact, it holds in all lattices with up to 3,337 elements, and it fails in a 3,338-element lattice.
- This identity could, in principle, be written explicitly. However, it would then fill a book.

A mystery

- Tautology: statement true everywhere (e.g., " $x * y = x * y$ ", " $x = y$ or $x \neq y$ ", etc.)

A mystery

- Tautology: statement true everywhere (e.g., " $x * y = x * y$ ", " $x = y$ or $x \neq y$ ", etc.)
- Set $x * y = x^3 + y^2$, for all integers (or real numbers, the problem is equivalent) x and y.

A mystery

- Tautology: statement true everywhere (e.g., " $x * y = x * y$ ", " $x = y$ or $x \neq y$ ", etc.)
- Set $x * y = x^3 + y^2$, for all integers (or real numbers, the problem is equivalent) x and y.
- Does there exist a non-tautological identity, satisfied by that operation $*$? (As far as I know, this problem was stated by Harvey Friedman in 1986, and it is still open; see also Roger Tian's 2009 arXiv preprint, https://arxiv.org/abs/0910.1571)

A mystery

- Tautology: statement true everywhere (e.g., " $x * y = x * y$ ", " $x = y$ or $x \neq y$ ", etc.)
- Set $x * y = x^3 + y^2$, for all integers (or real numbers, the problem is equivalent) x and y.
- Does there exist a non-tautological identity, satisfied by that operation $*$? (As far as I know, this problem was stated by Harvey Friedman in 1986, and it is still open; see also Roger Tian's 2009 arXiv preprint, https://arxiv.org/abs/0910.1571)
- Example of attempt: $x * y = x^3 + y^2$ is not identical to $y * x = x^2 + y^3$. Hence, the identity $x * y = y * x$ does not hold.

Thanks for your attention!