MAKING MANY MORE MATRIX MULTIPLICATION METHODS

Manuel Kauers · Institute for Algebra · JKU

Joint work with Marijn Heule (Texas) and Martina Seidl (Linz)

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{pmatrix}$$

$$c_{1,1} = a_{1,1} \cdot b_{1,1} + a_{1,2} \cdot b_{2,1}$$
$$c_{1,2} = a_{1,1} \cdot b_{1,2} + a_{1,2} \cdot b_{2,2}$$
$$c_{2,1} = a_{2,1} \cdot b_{1,1} + a_{2,2} \cdot b_{2,1}$$
$$c_{2,2} = a_{2,1} \cdot b_{1,2} + a_{2,2} \cdot b_{2,2}$$

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{pmatrix}$$

$$\begin{aligned} c_{1,1} &= M_1 + M_4 - M_5 + M_7 \\ c_{1,2} &= M_3 + M_5 \\ c_{2,1} &= M_2 + M_4 \\ c_{2,2} &= M_1 - M_2 + M_3 + M_6 \end{aligned}$$

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{pmatrix}$$

... where

$$\begin{aligned}
M_1 &= (a_{1,1} + a_{2,2}) \cdot (b_{1,1} + b_{2,2}) \\
M_2 &= (a_{2,1} + a_{2,2}) \cdot b_{1,1} \\
M_3 &= a_{1,1} \cdot (b_{1,2} - b_{2,2}) \\
M_4 &= a_{2,2} \cdot (b_{2,1} - b_{1,1}) \\
M_5 &= (a_{1,1} + a_{1,2}) \cdot b_{2,2} \\
M_6 &= (a_{2,1} - a_{1,1}) \cdot (b_{1,1} + b_{1,2}) \\
M_7 &= (a_{1,2} - a_{2,2}) \cdot (b_{2,1} + b_{2,2})
\end{aligned}$$

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{pmatrix}$$

- This scheme needs 7 multiplications instead of 8.

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{pmatrix}$$

- This scheme needs 7 multiplications instead of 8.
- Recursive application allows to multiply $n \times n$ matrices with $O(n^{\log_2 7})$ operations in the ground ring.

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{pmatrix}$$

- This scheme needs 7 multiplications instead of 8.
- Recursive application allows to multiply $n \times n$ matrices with $O(n^{\log_2 7})$ operations in the ground ring.
- Let ω be the smallest number so that $n \times n$ matrices can be multiplied using $O(n^{\omega})$ operations in the ground domain.

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{pmatrix}$$

- This scheme needs 7 multiplications instead of 8.
- Recursive application allows to multiply $n \times n$ matrices with $O(n^{\log_2 7})$ operations in the ground ring.
- Let ω be the smallest number so that $n \times n$ matrices can be multiplied using $O(n^{\omega})$ operations in the ground domain.
- Then $2 \leq \omega < 3$. What is the exact value?

- Strassen 1969: $\omega \leq \log_2 7 \leq 2.807$

- Strassen 1969: $\omega \leq \log_2 7 \leq 2.807$
- Pan 1978: $\omega \leq 2.796$
- Bini et al. 1979: $\omega \leq 2.7799$
- Schönhage 1981: $\omega \leq 2.522$
- Romani 1982: $\omega \leq 2.517$
- Coppersmith/Winograd 1981: $\omega \leq 2.496$
- Strassen 1986: $\omega \leq 2.479$
- Coppersmith/Winograd 1990: $\omega \leq 2.376$

- Strassen 1969: $\omega \le \log_2 7 \le 2.807$
- Pan 1978: $\omega \le 2.796$
- Bini et al. 1979: $\omega \le 2.7799$
- Schönhage 1981: $\omega \le 2.522$
- Romani 1982: $\omega \le 2.517$
- Coppersmith/Winograd 1981: $\omega \le 2.496$
- Strassen 1986: $\omega \le 2.479$
- Coppersmith/Winograd 1990: $\omega \le 2.376$
- Stothers 2010: $\omega \le 2.374$
- Williams 2011: $\omega \le 2.3728642$
- Le Gall 2014: $\omega \le 2.3728639$

- Only Strassen's algorithm beats the classical algorithm for reasonable problem sizes.

- Only Strassen's algorithm beats the classical algorithm for reasonable problem sizes.
- Want: a matrix multiplication algorithm that beats Strassen's algorithm for matrices of moderate size.

- Only Strassen's algorithm beats the classical algorithm for reasonable problem sizes.
- Want: a matrix multiplication algorithm that beats Strassen's algorithm for matrices of moderate size.
- Idea: instead of dividing the matrices into 2×2-block matrices, divide them into 3×3-block matrices.

- Only Strassen's algorithm beats the classical algorithm for reasonable problem sizes.
- Want: a matrix multiplication algorithm that beats Strassen's algorithm for matrices of moderate size.
- Idea: instead of dividing the matrices into 2×2-block matrices, divide them into 3×3-block matrices.
- Question: What's the minimal number of multiplications needed to multiply two 3×3 matrices?

- Only Strassen's algorithm beats the classical algorithm for reasonable problem sizes.
- Want: a matrix multiplication algorithm that beats Strassen's algorithm for matrices of moderate size.
- Idea: instead of dividing the matrices into 2×2-block matrices, divide them into 3×3-block matrices.
- Question: What's the minimal number of multiplications needed to multiply two 3×3 matrices?
- Answer: Nobody knows.

Question: What's the minimal number of multiplications needed to multiply two 3×3 matrices?

Question: What's the minimal number of multiplications needed to multiply two 3×3 matrices?

- naive algorithm: 27

Question: What's the minimal number of multiplications needed to multiply two 3×3 matrices?

- naive algorithm: 27
- padd with zeros, use Strassen twice, cleanup: 25

Question: What's the minimal number of multiplications needed to multiply two 3×3 matrices?

- naive algorithm: 27
- padd with zeros, use Strassen twice, cleanup: 25
- best known upper bound: 23 (Laderman 1976)

Question: What's the minimal number of multiplications needed to multiply two 3×3 matrices?

- naive algorithm: 27
- padd with zeros, use Strassen twice, cleanup: 25
- best known upper bound: 23 (Laderman 1976)
- best known lower bound: 19 (Bläser 2003)

Question: What's the minimal number of multiplications needed to multiply two 3×3 matrices?

- naive algorithm: 27
- padd with zeros, use Strassen twice, cleanup: 25
- best known upper bound: 23 (Laderman 1976)
- best known lower bound: 19 (Bläser 2003)
- maximal number of multiplications allowed if we want to beat Strassen: 21 (because $\log_3 21 < \log_2 7 < \log_3 22$).

- While Strassen's scheme is essentially the only way to do the 2×2 case with 7 multiplications, there are several distinct schemes for 3×3 matrices using 23 multiplications.

- While Strassen's scheme is essentially the only way to do the 2×2 case with 7 multiplications, there are several distinct schemes for 3×3 matrices using 23 multiplications.
- In fact, there are infinitely many such schemes due to Johnson and McLoughlin, but they involve fractional coefficients and therefore do not work for every coefficient ring.

- While Strassen's scheme is essentially the only way to do the 2×2 case with 7 multiplications, there are several distinct schemes for 3×3 matrices using 23 multiplications.
- In fact, there are infinitely many such schemes due to Johnson and McLoughlin, but they involve fractional coefficients and therefore do not work for every coefficient ring.
- If we insist in integer coefficients, there have so far (and to our knowledge) been only three other schemes for 3×3 matrices and 23 multiplications.

- While Strassen's scheme is essentially the only way to do the 2×2 case with 7 multiplications, there are several distinct schemes for 3×3 matrices using 23 multiplications.
- In fact, there are infinitely many such schemes due to Johnson and McLoughlin, but they involve fractional coefficients and therefore do not work for every coefficient ring.
- If we insist in integer coefficients, there have so far (and to our knowledge) been only three other schemes for 3×3 matrices and 23 multiplications.
- Using altogether about 35 years of computation time, we found more than 13000 new schemes for 3×3 and 23, and we expect that there are many others.

- While Strassen's scheme is essentially the only way to do the 2×2 case with 7 multiplications, there are several distinct schemes for 3×3 matrices using 23 multiplications.
- In fact, there are infinitely many such schemes due to Johnson and McLoughlin, but they involve fractional coefficients and therefore do not work for every coefficient ring.
- If we insist in integer coefficients, there have so far (and to our knowledge) been only three other schemes for 3×3 matrices and 23 multiplications.
- Using altogether about 35 years of computation time, we found more than 13000 new schemes for 3×3 and 23, and we expect that there are many others.
- Unfortunately we found no scheme with only 22 multiplications

How to search for a matrix multiplication scheme?

How to search for a matrix multiplication scheme?

Make an ansatz

$$\begin{aligned}
M_1 &= (\alpha_{1,1}^{(1)} a_{1,1} + \alpha_{1,2}^{(1)} a_{1,2} + \cdots)(\beta_{1,1}^{(1)} b_{1,1} + \cdots) \\
M_2 &= (\alpha_{1,1}^{(2)} a_{1,1} + \alpha_{1,2}^{(2)} a_{1,2} + \cdots)(\beta_{1,1}^{(2)} b_{1,1} + \cdots) \\
&\vdots \\
c_{1,1} &= \gamma_{1,1}^{(1)} M_1 + \gamma_{1,1}^{(2)} M_2 + \cdots \\
&\vdots
\end{aligned}$$

How to search for a matrix multiplication scheme?

Make an ansatz

$$
\begin{aligned}
M_1 &= (\alpha_{1,1}^{(1)} a_{1,1} + \alpha_{1,2}^{(1)} a_{1,2} + \cdots)(\beta_{1,1}^{(1)} b_{1,1} + \cdots) \\
M_2 &= (\alpha_{1,1}^{(2)} a_{1,1} + \alpha_{1,2}^{(2)} a_{1,2} + \cdots)(\beta_{1,1}^{(2)} b_{1,1} + \cdots) \\
&\vdots \\
c_{1,1} &= \gamma_{1,1}^{(1)} M_1 + \gamma_{1,1}^{(2)} M_2 + \cdots \\
&\vdots
\end{aligned}
$$

Set $c_{i,j} = \sum_k a_{i,k} b_{k,j}$ for all i, j and compare coefficients.

How to search for a matrix multiplication scheme?

This gives the Brent equations (e.g., for 3×3 with 23 multiplications)

$$\forall\, i, j, k, l, m, n \in \{1, 2, 3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k} \delta_{i,m} \delta_{l,n}$$

How to search for a matrix multiplication scheme?

This gives the Brent equations (e.g., for 3×3 with 23 multiplications)

$$\forall\ i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- $3^6 = 729$ cubic equations
- $23 \cdot 9 \cdot 3 = 621$ variables

How to search for a matrix multiplication scheme?

This gives the Brent equations (e.g., for 3×3 with 23 multiplications)

$$\forall\ i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- $3^6 = 729$ cubic equations
- $23 \cdot 9 \cdot 3 = 621$ variables

Laderman claims that he solved this system by hand,
but he doesn't say exactly how.

How to search for a matrix multiplication scheme?

This gives the Brent equations (e.g., for 3×3 with 23 multiplications)

$$\forall\ i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- $3^6 = 729$ cubic equations
- $23 \cdot 9 \cdot 3 = 621$ variables

Laderman claims that he solved this system by hand,
but he doesn't say exactly how.

Idea: Solve this system in $\mathbb{Z}_2$.

How to search for a matrix multiplication scheme?

This gives the Brent equations (e.g., for 3×3 with 23 multiplications)

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- $3^6 = 729$ cubic equations
- $23 \cdot 9 \cdot 3 = 621$ variables

Laderman claims that he solved this system by hand,
but he doesn't say exactly how.

Idea: Solve this system in $\mathbb{Z}_2$.

Reading $\alpha_{i,j}^{(q)}$, $\beta_{k,l}^{(q)}$, $\gamma_{m,n}^{(q)}$ as boolean variables and $+$ as XOR, the problem becomes a SAT problem.

How to search for a matrix multiplication scheme?

This gives the Brent equations (e.g., for 3×3 with 23 multiplications)

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

Modern SAT solvers are extremely powerful, but this formula happens to be very hard for them nevertheless. We need to support them in various ways (no time to explain how exactly.)

How to search for a matrix multiplication scheme?

This gives the Brent equations (e.g., for 3×3 with 23 multiplications)

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

Modern SAT solvers are extremely powerful, but this formula happens to be very hard for them nevertheless. We need to support them in various ways (no time to explain how exactly.)

With the appropriate assistance, and by using our large computers, we are able to find several solutions per minute.

How to search for a matrix multiplication scheme?

This gives the Brent equations (e.g., for 3×3 with 23 multiplications)

$$\forall\ i,j,k,l,m,n \in \{1,2,3\}: \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

Modern SAT solvers are extremely powerful, but this formula happens to be very hard for them nevertheless. We need to support them in various ways (no time to explain how exactly.)

With the appropriate assistance, and by using our large computers, we are able to find several solutions per minute.

Are all these solutions new? What does it to be a new solution?

Matrix multiplication $AB = C$ enjoys several symmetries:

Matrix multiplication $AB = C$ enjoys several symmetries:

- $AUU^{-1}B = C$ for every invertible U

Matrix multiplication $AB = C$ enjoys several symmetries:

- $AUU^{-1}B = C$ for every invertible U
- $VAB = VC$ for every invertible V

Matrix multiplication $AB = C$ enjoys several symmetries:

- $AUU^{-1}B = C$ for every invertible U
- $VAB = VC$ for every invertible V
- $ABW = CW$ for every invertible W

Matrix multiplication $AB = C$ enjoys several symmetries:

- $AUU^{-1}B = C$ for every invertible U
- $VAB = VC$ for every invertible V
- $ABW = CW$ for every invertible W
- $B^\top A^\top = C^\top$

Matrix multiplication $AB = C$ enjoys several symmetries:

- $AUU^{-1}B = C$ for every invertible U
- $VAB = VC$ for every invertible V
- $ABW = CW$ for every invertible W
- $B^\top A^\top = C^\top$
- and one more that is a little more subtle

Matrix multiplication $AB = C$ enjoys several symmetries:

- $AUU^{-1}B = C$ for every invertible U
- $VAB = VC$ for every invertible V
- $ABW = CW$ for every invertible W
- $B^\top A^\top = C^\top$
- and one more that is a little more subtle

The symmetry group turns out to be $S_3 \times \mathrm{GL}(n)^3$.

Matrix multiplication $AB = C$ enjoys several symmetries:

- $AUU^{-1}B = C$ for every invertible U
- $VAB = VC$ for every invertible V
- $ABW = CW$ for every invertible W
- $B^\top A^\top = C^\top$
- and one more that is a little more subtle

Taking also into account that we can reorder the sums in the Brent equations, the symmetry group is in fact $S_{23} \times S_3 \times \mathrm{GL}(n)^3$.

Matrix multiplication $AB = C$ enjoys several symmetries:

- $AUU^{-1}B = C$ for every invertible U
- $VAB = VC$ for every invertible V
- $ABW = CW$ for every invertible W
- $B^\top A^\top = C^\top$
- and one more that is a little more subtle

Taking also into account that we can reorder the sums in the Brent equations, the symmetry group is in fact $S_{23} \times S_3 \times \mathrm{GL}(n)^3$.

For $\mathbb{Z}_2$, this group has almost 10^{30} elements. For comparison: the whole search space has size $2^{621} \approx 10^{187}$.

Matrix multiplication $AB = C$ enjoys several symmetries:

- $AUU^{-1}B = C$ for every invertible U
- $VAB = VC$ for every invertible V
- $ABW = CW$ for every invertible W
- $B^\top A^\top = C^\top$
- and one more that is a little more subtle

Taking also into account that we can reorder the sums in the Brent equations, the symmetry group is in fact $S_{23} \times S_3 \times \mathrm{GL}(n)^3$.

Group elements can map solutions into other solutions. A solution is new when it cannot be mapped to one we have seen before.

Matrix multiplication $AB = C$ enjoys several symmetries:

- $AUU^{-1}B = C$ for every invertible U
- $VAB = VC$ for every invertible V
- $ABW = CW$ for every invertible W
- $B^\top A^\top = C^\top$
- and one more that is a little more subtle

Taking also into account that we can reorder the sums in the Brent equations, the symmetry group is in fact $S_{23} \times S_3 \times \mathrm{GL}(n)^3$.

Group elements can map solutions into other solutions. A solution is new when it cannot be mapped to one we have seen before.

The 13000 new schemes announced earlier are new in this sense.

Lifting: How to get back from $\mathbb{Z}_2$ to $\mathbb{Z}$?

Remember the Brent equations:

$$\forall\ i, j, k, l, m, n \in \{1, 2, 3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

Lifting: How to get back from $\mathbb{Z}_2$ to $\mathbb{Z}$?

Remember the Brent equations:

$$\forall\ i, j, k, l, m, n \in \{1, 2, 3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k} \delta_{i,m} \delta_{l,n}$$

- Suppose we know a solution in $\mathbb{Z}_2$.

Lifting: How to get back from $\mathbb{Z}_2$ to $\mathbb{Z}$?

Remember the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- Suppose we know a solution in $\mathbb{Z}_2$.
- Assume it came from a solution with coefficients $0, \pm 1 \in \mathbb{Z}$.

Lifting: How to get back from $\mathbb{Z}_2$ to $\mathbb{Z}$?

Remember the Brent equations:

$$\forall\ i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- Suppose we know a solution in $\mathbb{Z}_2$.
- Assume it came from a solution with coefficients $0, \pm 1 \in \mathbb{Z}$.
- Then each $0 \in \mathbb{Z}_2$ was $0 \in \mathbb{Z}$ and each $1 \in \mathbb{Z}_2$ was $\pm 1 \in \mathbb{Z}$.

Lifting: How to get back from $\mathbb{Z}_2$ to $\mathbb{Z}$?

Remember the Brent equations:

$$\forall\ i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- Suppose we know a solution in $\mathbb{Z}_2$.
- Assume it came from a solution with coefficients $0, \pm 1 \in \mathbb{Z}$.
- Then each $0 \in \mathbb{Z}_2$ was $0 \in \mathbb{Z}$ and each $1 \in \mathbb{Z}_2$ was $\pm 1 \in \mathbb{Z}$.
- Plug the 0s of the $\mathbb{Z}_2$-solution into the Brent equations.

Lifting: How to get back from $\mathbb{Z}_2$ to $\mathbb{Z}$?

Remember the Brent equations:

$$\forall\, i, j, k, l, m, n \in \{1, 2, 3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- Suppose we know a solution in $\mathbb{Z}_2$.
- Assume it came from a solution with coefficients $0, \pm 1 \in \mathbb{Z}$.
- Then each $0 \in \mathbb{Z}_2$ was $0 \in \mathbb{Z}$ and each $1 \in \mathbb{Z}_2$ was $\pm 1 \in \mathbb{Z}$.
- Plug the 0s of the $\mathbb{Z}_2$-solution into the Brent equations.
- For each remaining variable x, add a new equation $x^2 - 1$.

Lifting: How to get back from $\mathbb{Z}_2$ to $\mathbb{Z}$?

Remember the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- Suppose we know a solution in $\mathbb{Z}_2$.
- Assume it came from a solution with coefficients $0, \pm 1 \in \mathbb{Z}$.
- Then each $0 \in \mathbb{Z}_2$ was $0 \in \mathbb{Z}$ and each $1 \in \mathbb{Z}_2$ was $\pm 1 \in \mathbb{Z}$.
- Plug the 0s of the $\mathbb{Z}_2$-solution into the Brent equations.
- For each remaining variable x, add a new equation $x^2 - 1$.
- Solve the resulting nonlinear system over $\mathbb{Q}$.

Lifting: How to get back from $\mathbb{Z}_2$ to $\mathbb{Z}$?

Remember the Brent equations:

$$\forall\ i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- Can every $\mathbb{Z}_2$-solution be lifted to a $\mathbb{Z}$-solution in this way?

Lifting: How to get back from $\mathbb{Z}_2$ to $\mathbb{Z}$?

Remember the Brent equations:

$$\forall\ i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- Can every $\mathbb{Z}_2$-solution be lifted to a $\mathbb{Z}$-solution in this way?
- No, and we found some which don't admit a lifting.

Lifting: How to get back from $\mathbb{Z}_2$ to $\mathbb{Z}$?

Remember the Brent equations:

$$\forall\ i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- Can every $\mathbb{Z}_2$-solution be lifted to a $\mathbb{Z}$-solution in this way?
- No, and we found some which don't admit a lifting.
- But they are very rare. In almost all cases, the lifting succeeds.

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\ i, j, k, l, m, n \in \{1, 2, 3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k} \delta_{i,m} \delta_{l,n}$$

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- If we forget the values of $\alpha_{i,j}^{(q)}$, we can recover them by solving a linear system.

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- If we forget the values of $\beta_{k,l}^{(q)}$, we can recover them by solving a linear system.

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- If we forget the values of $\gamma_{m,n}^{(q)}$, we can recover them by solving a linear system.

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\, i, j, k, l, m, n \in \{1, 2, 3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- If we forget the values of $\gamma_{m,n}^{(q)}$, we can recover them by solving a linear system.

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- If we forget the values of $\gamma_{m,n}^{(q)}$, we can recover them by solving a linear system.
- This computation often gives nontrivial affine spaces of solutions, i.e., more general schemes involving free parameters.

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- If we forget the values of $\gamma_{m,n}^{(q)}$, we can recover them by solving a linear system.
- This computation often gives nontrivial affine spaces of solutions, i.e., more general schemes involving free parameters.
- In fact, for every $q \in \{1,\dots,23\}$ we can independently set replace all $\alpha_{i,j}^{(q)}$ or all $\beta_{k,l}^{(q)}$ or all $\gamma_{m,n}^{(q)}$ by unknowns.

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- If we forget the values of $\gamma_{m,n}^{(q)}$, we can recover them by solving a linear system.
- This computation often gives nontrivial affine spaces of solutions, i.e., more general schemes involving free parameters.
- In fact, for every $q \in \{1,\dots,23\}$ we can independently set replace all $\alpha_{i,j}^{(q)}$ or all $\beta_{k,l}^{(q)}$ or all $\gamma_{m,n}^{(q)}$ by unknowns.
- Playing the game repeatedly with various choices, we introduce more and more free parameters into the schemes.

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- We found several families with up to 17 parameters and with coefficients in $\mathbb{Z}$.

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- We found several families with up to 17 parameters and with coefficients in $\mathbb{Z}$.
- Gröbner bases computations can be used to check that these parameters are really independent.

Clustering: Turning each solution into many additional ones.

Suppose we have a solution of the Brent equations:

$$\forall\, i,j,k,l,m,n \in \{1,2,3\} : \sum_{q=1}^{23} \alpha_{i,j}^{(q)} \beta_{k,l}^{(q)} \gamma_{m,n}^{(q)} = \delta_{j,k}\delta_{i,m}\delta_{l,n}$$

- We found several families with up to 17 parameters and with coefficients in $\mathbb{Z}$.
- Gröbner bases computations can be used to check that these parameters are really independent.
- For comparison: The schemes of Johnson and McLoughlin had only 3 parameters and coefficients in $\mathbb{Q}$.

So what?

So what?

- Okay, so there are many more matrix multiplication methods for 3×3 matrices with 23 coefficient multiplications than previously known.

So what?

- Okay, so there are many more matrix multiplication methods for 3×3 matrices with 23 coefficient multiplications than previously known.
- In fact, we have shown that the dimension of the algebraic set defined by the Brent equation is much larger than was previously known.

So what?

- Okay, so there are many more matrix multiplication methods for 3×3 matrices with 23 coefficient multiplications than previously known.
- In fact, we have shown that the dimension of the algebraic set defined by the Brent equation is much larger than was previously known.
- But none of this has any immediate implications on the complexity of matrix multiplication, neither theoretically nor practically.

So what?

- Okay, so there are many more matrix multiplication methods for 3×3 matrices with 23 coefficient multiplications than previously known.
- In fact, we have shown that the dimension of the algebraic set defined by the Brent equation is much larger than was previously known.
- But none of this has any immediate implications on the complexity of matrix multiplication, neither theoretically nor practically.
- In particular, it remains open whether there is a multiplication method for 3×3 matrices with 22 coefficient multiplications. If you find one, let us know.

Check out our website for browsing through the schemes and families we found:

http://www.algebra.uni-linz.ac.at/research/matrix-multiplication/