On fast multiplication of a matrix by its transpose

Jean-Guillaume Dumas Clément Pernet Alexandre Sedoglavic

July 22. 2020
ISSAC

Outline

2×2 matrix multiplication

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \times \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} (A_{11}B_{11} + A_{12}B_{21}) & (A_{11}B_{12} + A_{12}B_{22}) \\ (A_{21}B_{11} + A_{22}B_{21}) & (A_{21}B_{12} + A_{22}B_{22}) \end{bmatrix} = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}$$

Classical Algorithm

8 multiplications, 4 additions

2×2 matrix multiplication

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \times \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} (A_{11}B_{11} + A_{12}B_{21}) & (A_{11}B_{12} + A_{12}B_{22}) \\ (A_{21}B_{11} + A_{22}B_{21}) & (A_{21}B_{12} + A_{22}B_{22}) \end{bmatrix} = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}$$

Classical Algorithm

8 multiplications, 4 additions

[Strassen 1969]

7 multiplications, 18 additions

2×2 matrix multiplication

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \times \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} (A_{11}B_{11} + A_{12}B_{21}) & (A_{11}B_{12} + A_{12}B_{22}) \\ (A_{21}B_{11} + A_{22}B_{21}) & (A_{21}B_{12} + A_{22}B_{22}) \end{bmatrix} = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}$$

Classical Algorithm

8 multiplications, 4 additions

[Strassen 1969]
7 multiplications, 18 additions

[Winograd 1973? 1977]
7 multiplications, 15 additions

2×2 matrix multiplication

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \times \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} (A_{11}B_{11} + A_{12}B_{21}) & (A_{11}B_{12} + A_{12}B_{22}) \\ (A_{21}B_{11} + A_{22}B_{21}) & (A_{21}B_{12} + A_{22}B_{22}) \end{bmatrix} = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}$$

Classical Algorithm

8 multiplications, 4 additions

[Strassen 1969]
7 multiplications, 18 additions

[Winograd 1973? 1977]
7 multiplications, 15 additions

[Hopcroft-Kerr 1969]: 7 multiplications minimum

[Bshouty 1995]: 15 additions minimum
(for a bilin. alg. with 7 mult.)

Matrix multiplication by its transpose $A \cdot A^T$

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \times \begin{bmatrix} A_{11}^T & A_{21}^T \\ A_{12}^T & A_{22}^T \end{bmatrix} = \begin{bmatrix} (A_{11}A_{11}^T + A_{12}A_{12}^T) & \\ (A_{21}A_{11}^T + A_{22}A_{12}^T) & (A_{21}A_{21}^T + A_{22}A_{22}^T) \end{bmatrix} = \begin{bmatrix} C_{11} & \boxed{C_{21}^T} \\ C_{21} & C_{22} \end{bmatrix}$$

Divide & Conquer Algorithm

6 multiplications, 3 additions

Matrix multiplication by its transpose $A \cdot A^{\mathsf{T}}$

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \times \begin{bmatrix} A_{11}^{\mathsf{T}} & A_{21}^{\mathsf{T}} \\ A_{12}^{\mathsf{T}} & A_{22}^{\mathsf{T}} \end{bmatrix} = \begin{bmatrix} (A_{11}A_{11}^{\mathsf{T}} + A_{12}A_{12}^{\mathsf{T}}) & \\ (A_{21}A_{11}^{\mathsf{T}} + A_{22}A_{12}^{\mathsf{T}}) & (A_{21}A_{21}^{\mathsf{T}} + A_{22}A_{22}^{\mathsf{T}}) \end{bmatrix} = \begin{bmatrix} C_{11} & \boxed{C_{21}^{\mathsf{T}}} \\ C_{21} & C_{22} \end{bmatrix}$$

Divide & Conquer Algorithm

6 multiplications, 3 additions

here (over $\mathbb{C}$ & over any field in > 0 characteristic)

5 multiplications, 7.5 additions

Outline

From Strassen-Winograd multiplication algorithm

Require: $A = \left[\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{smallmatrix}\right]$;
Ensure: $C = A \cdot B$

1. 8 additions:

$$\begin{array}{llll} s_1 \leftarrow a_{11} - a_{21}, & s_2 \leftarrow a_{21} + a_{22}, & s_3 \leftarrow s_2 - a_{11}, & s_4 \leftarrow a_{12} - s_3, \\ t_1 \leftarrow b_{22} - b_{12}, & t_2 \leftarrow b_{12} - b_{11}, & t_3 \leftarrow b_{11} + t_1, & t_4 \leftarrow b_{21} - t_3. \end{array}$$

2. 7 recursive multiplications:

$$\begin{array}{llll} p_1 \leftarrow a_{11} \cdot b_{11}, & p_2 \leftarrow a_{12} \cdot b_{21}, & p_3 \leftarrow a_{22} \cdot t_4, & p_4 \leftarrow s_1 \cdot t_1, \\ & p_5 \leftarrow s_3 \cdot t_3, & p_6 \leftarrow s_4 \cdot b_{22}, & p_7 \leftarrow s_2 \cdot t_2. \end{array}$$

3. 7 final additions:

$$\begin{array}{llll} c_1 \leftarrow p_1 + p_5, & c_2 \leftarrow c_1 + p_4, & c_3 \leftarrow p_1 + p_2, & c_4 \leftarrow c_2 + p_3, \\ c_5 \leftarrow c_2 + p_7, & & c_6 \leftarrow c_1 + p_7, & c_7 \leftarrow c_6 + p_6. \end{array}$$

4. **return** $C = \left[\begin{smallmatrix} c_3 & c_7 \\ c_4 & c_5 \end{smallmatrix}\right]$.

. . . to its specialization to $A \cdot A^{\mathsf{T}}$ . . .

Require: $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ with $A^{\mathsf{T}} = \begin{bmatrix} a_{11}^{\mathsf{T}} & a_{21}^{\mathsf{T}} \\ a_{12}^{\mathsf{T}} & a_{22}^{\mathsf{T}} \end{bmatrix}$;

Ensure: $C = A \cdot A^{\mathsf{T}}$

1. 6 additions:

$$s_1 \leftarrow a_{11} - a_{21}, \quad s_2 \leftarrow a_{21} + a_{22}, \quad s_3 \leftarrow s_2 - a_{11}, \quad \cancel{s_4 \leftarrow a_{12} - s_3},$$
$$t_1 \leftarrow a_{22}^{\mathsf{T}} - a_{21}^{\mathsf{T}}, \quad \cancel{t_2 \leftarrow a_{21}^{\mathsf{T}} - a_{11}^{\mathsf{T}}}, \quad t_3 \leftarrow a_{11}^{\mathsf{T}} + t_1, \quad t_4 \leftarrow a_{12}^{\mathsf{T}} - t_3.$$

2. 6 multiplications (2 recursive, 4 general):

$$p_1 \leftarrow a_{11} \cdot a_{11}^{\mathsf{T}}, \quad p_2 \leftarrow a_{12} \cdot a_{12}^{\mathsf{T}}, \quad p_3 \leftarrow a_{22} \cdot t_4, \quad p_4 \leftarrow s_1 \cdot t_1,$$
$$p_5 \leftarrow s_3 \cdot t_3, \quad \cancel{p_6 \leftarrow s_4 \cdot a_{22}^{\mathsf{T}}}, \quad p_7 \leftarrow s_2 \cdot \boxed{s_1^{\mathsf{T}}}.$$

3. 5 final additions:

$$c_1 \leftarrow p_1 + p_5, \quad c_2 \leftarrow c_1 + p_4, \quad c_3 \leftarrow p_1 + p_2, \quad c_4 \leftarrow c_2 + p_3,$$
$$c_5 \leftarrow c_2 - p_7, \quad \cancel{c_6 \leftarrow c_1 - p_7}, \quad \cancel{c_7 \leftarrow c_6 + p_6}.$$

4. **return** $C = \begin{bmatrix} c_3 & \cancel{c_7} \\ c_4 & c_5 \end{bmatrix}$.

. . . to its specialization to $A \cdot A^{\mathsf{T}}$ . . .

Require: $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ with $A^{\mathsf{T}} = \begin{bmatrix} a_{11}^{\mathsf{T}} & a_{21}^{\mathsf{T}} \\ a_{12}^{\mathsf{T}} & a_{22}^{\mathsf{T}} \end{bmatrix}$;

Ensure: $C = A \cdot A^{\mathsf{T}}$

☹ all variants have sign discrepancies

1. 6 additions:

$$s_1 \leftarrow a_{11} - a_{21}, \quad s_2 \leftarrow a_{21} + a_{22}, \quad s_3 \leftarrow s_2 - a_{11}, \quad \cancel{s_4 \leftarrow a_{12} - s_3},$$
$$t_1 \leftarrow a_{22}^{\mathsf{T}} - a_{21}^{\mathsf{T}}, \quad \cancel{t_2 \leftarrow a_{21}^{\mathsf{T}} - a_{11}^{\mathsf{T}}}, \quad t_3 \leftarrow a_{11}^{\mathsf{T}} + t_1, \quad t_4 \leftarrow a_{12}^{\mathsf{T}} - t_3.$$

2. 6 multiplications (2 recursive, 4 general):

$$p_1 \leftarrow a_{11} \cdot a_{11}^{\mathsf{T}}, \quad p_2 \leftarrow a_{12} \cdot a_{12}^{\mathsf{T}}, \quad p_3 \leftarrow a_{22} \cdot t_4, \quad p_4 \leftarrow s_1 \cdot t_1,$$
$$p_5 \leftarrow s_3 \cdot t_3, \quad \cancel{p_6 \leftarrow s_4 \cdot a_{22}^{\mathsf{T}}}, \quad p_7 \leftarrow s_2 \cdot \boxed{s_1^{\mathsf{T}}}.$$

3. 5 final additions:

$$c_1 \leftarrow p_1 + p_5, \quad c_2 \leftarrow c_1 + p_4, \quad c_3 \leftarrow p_1 + p_2, \quad c_4 \leftarrow c_2 + p_3,$$
$$c_5 \leftarrow c_2 - p_7, \quad \cancel{c_6 \leftarrow c_1 - p_7}, \quad \cancel{c_7 \leftarrow c_6 + p_6}.$$

4. **return** $C = \begin{bmatrix} c_3 & \cancel{c_7} \\ c_4 & c_5 \end{bmatrix}$.

. . . with a parameterized algorithm

Require: $A = \left[\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right]$ and Y s.t. $\boxed{YY^{\mathsf{T}} = -\mathrm{I}_{n/2}}$;

Ensure: $C = A \cdot A^{\mathsf{T}}$

1. 4 additions and 2 multiplications by Y:

$$s_1 \leftarrow (a_{21} - a_{11})\boxed{Y}, \quad \cancel{s_2 \leftarrow a_{22} - a_{21}\boxed{Y}, \quad t_2 \leftarrow \boxed{Y^{\mathsf{T}}}(a_{21}^{\mathsf{T}} - a_{11}^{\mathsf{T}})} \quad \cancel{s_3 \leftarrow s_1 - a_{22}. \quad t_3 \leftarrow t_2 - a_{22}^{\mathsf{T}}} \quad \cancel{s_4 \leftarrow s_3 + a_{12}, \quad t_4 \leftarrow t_3 + a_{12}^{\mathsf{T}}}$$

2. 5 multiplications (3 recursive, 2 general):

$$p_1 \leftarrow a_{11} \cdot a_{11}^{\mathsf{T}}, \quad p_2 \leftarrow a_{12} \cdot a_{12}^{\mathsf{T}}, \quad p_3 \leftarrow a_{22} \cdot \boxed{s_4^{\mathsf{T}}}, \quad p_4 \leftarrow s_1 \cdot \boxed{s_2^{\mathsf{T}}},$$
$$p_5 \leftarrow s_3 \cdot \boxed{s_3^{\mathsf{T}}}. \quad \cancel{p_7 \leftarrow s_2 \cdot s_1^{\mathsf{T}}}$$

3. 5 final additions:

$$c_1 \leftarrow p_1 + p_5, \quad c_2 \leftarrow c_1 + p_4, \quad c_3 \leftarrow p_1 + p_2, \quad c_4 \leftarrow c_2 + p_3,$$
$$c_5 \leftarrow c_2 + \boxed{p_4^{\mathsf{T}}}.$$

4. **return** $C = \left[\begin{smallmatrix} c_3 & \\ c_4 & c_5 \end{smallmatrix}\right]$.

Fast algorithm for $A \cdot A^{\mathsf{T}}$ exploiting symmetries

Require: $A = \left[\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right]$ and Y s.t. $YY^{\mathsf{T}} = -\mathrm{I}_{n/2}$;
Ensure: $C = A \cdot A^{\mathsf{T}}$

1. 4 additions and 2 multiplications by Y:

$$s_1 \leftarrow (a_{21} - a_{11})Y, \quad s_2 \leftarrow a_{22} - a_{21}Y, \quad s_3 \leftarrow s_1 - a_{22}. \quad s_4 \leftarrow s_3 + a_{12},$$

2. 5 multiplications (3 recursive, 2 general):

$$p_1 \leftarrow a_{11} \cdot a_{11}^{\mathsf{T}}, \quad p_2 \leftarrow a_{12} \cdot a_{12}^{\mathsf{T}}, \quad p_3 \leftarrow a_{22} \cdot s_4^{\mathsf{T}}, \quad p_4 \leftarrow s_1 \cdot s_2^{\mathsf{T}},$$
$$p_5 \leftarrow s_3 \cdot s_3^{\mathsf{T}}.$$

3. 2 complete and 3 symmetric additions:

$$\boxed{Low(c_1) \leftarrow Low(p_1) + Low(p_5)}, \quad c_2 \leftarrow c_1 + p_4, \quad \boxed{Low(c_3) \leftarrow Low(p_1) + Low(p_2)},$$
$$\boxed{Low(c_5) \leftarrow Low(c_2) + Low(p_4^{\mathsf{T}})}, \quad c_4 \leftarrow c_2 + p_3.$$

4. **return** $C = \left[\begin{smallmatrix} c_3 & \\ c_4 & c_5 \end{smallmatrix}\right]$.

Outline

Skew orthogonal matrices?

Definition (Skew orthogonal matrix)

Y such that $Y \cdot Y^{\mathsf{T}} = -\mathrm{I}_n$

Skew orthogonal matrices?

Definition (Skew orthogonal matrix)

Y such that $Y \cdot Y^{\mathsf{T}} = -\mathrm{I}_n$

✓ $\mathbb{C}$: $Y = i \cdot \mathrm{I}_n$ ➡ no-op: swap real/imaginary & 1 sign

Skew orthogonal matrices?

Definition (Skew orthogonal matrix)

Y such that $Y \cdot Y^{\mathsf{T}} = -\mathrm{I}_n$

✓ $\mathbb{C}$: $Y = i \cdot \mathrm{I}_n$

✗ $\mathbb{R}$

➡ no-op: swap real/imaginary & 1 sign

Skew orthogonal matrices?

Definition (Skew orthogonal matrix)

Y such that $Y \cdot Y^{\mathsf{T}} = -\mathrm{I}_n$

- ✓ $\mathbb{C}$: $Y = i \cdot \mathrm{I}_n$
- ✗ $\mathbb{R}$
- ✗ $\mathbb{Q}$

➡ no-op: swap real/imaginary & 1 sign

Skew orthogonal matrices?

Definition (Skew orthogonal matrix)

Y such that $Y \cdot Y^{\mathsf{T}} = -\mathrm{I}_n$

- ✓ $\mathbb{C}$: $Y = i \cdot \mathrm{I}_n$ ➡ no-op: swap real/imaginary & 1 sign
- ✗ $\mathbb{R}$
- ✗ $\mathbb{Q}$
- ✓ characteristic 2 $\boxed{1 = -1 \text{ is a square}}$: ➡ $Y = \mathrm{I}_n$

Skew orthogonal matrices?

Definition (Skew orthogonal matrix)

Y such that $Y \cdot Y^{\mathsf{T}} = -\mathrm{I}_n$

- ✓ $\mathbb{C}$: $Y = i \cdot \mathrm{I}_n$ ➡ no-op: swap real/imaginary & 1 sign
- ✗ $\mathbb{R}$
- ✗ $\mathbb{Q}$
- ✓ characteristic 2 $\boxed{1 = -1 \text{ is a square}}$: ➡ $Y = \mathrm{I}_n$
- ✓ $\mathbb{K} \supseteq \mathbb{F}_{p^k}$: $(p \equiv 1 \mod 4)$ or $(k$ even$)$ then $\boxed{-1 \text{ is a square}}$ ➡ $Y = i \cdot \mathrm{I}_n$

Skew orthogonal matrices?

Definition (Skew orthogonal matrix)

Y such that $Y \cdot Y^{\mathsf{T}} = -\mathrm{I}_n$

- ✓ $\mathbb{C}$: $Y = i \cdot \mathrm{I}_n$ ➡ no-op: swap real/imaginary & 1 sign
- ✗ $\mathbb{R}$
- ✗ $\mathbb{Q}$
- ✓ characteristic 2 $\boxed{1 = -1 \text{ is a square}}$: ➡ $Y = \mathrm{I}_n$
- ✓ $\mathbb{K} \supseteq \mathbb{F}_{p^k}$: $(p \equiv 1 \mod 4)$ or $(k$ even$)$ then $\boxed{-1 \text{ is a square}}$ ➡ $Y = i \cdot \mathrm{I}_n$
- ✓ Other fields with positive characteristic, $n \geqslant 4$: $Y = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \otimes \mathrm{I}_{n/2} = \begin{pmatrix} a\,\mathrm{I}_{n/2} & b\,\mathrm{I}_{n/2} \\ -b\,\mathrm{I}_{n/2} & a\,\mathrm{I}_{n/2} \end{pmatrix} \in \mathbb{F}_q^{n \times n}$

Skew orthogonal matrices?

Definition (Skew orthogonal matrix)

Y such that $Y \cdot Y^{\mathsf{T}} = -\mathrm{I}_n$

- ✓ $\mathbb{C}$: $Y = i \cdot \mathrm{I}_n$ ➡ no-op: swap real/imaginary & 1 sign
- ✗ $\mathbb{R}$
- ✗ $\mathbb{Q}$
- ✓ characteristic 2 $\boxed{1 = -1 \text{ is a square}}$: ➡ $Y = \mathrm{I}_n$
- ✓ $\mathbb{K} \supseteq \mathbb{F}_{p^k}$: $(p \equiv 1 \mod 4)$ or $(k$ even$)$ then $\boxed{-1 \text{ is a square}}$ ➡ $Y = i \cdot \mathrm{I}_n$
- ✓ Other fields with positive characteristic, $n \geqslant 4$: $Y = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \otimes \mathrm{I}_{n/2} = \begin{pmatrix} a\,\mathrm{I}_{n/2} & b\,\mathrm{I}_{n/2} \\ -b\,\mathrm{I}_{n/2} & a\,\mathrm{I}_{n/2} \end{pmatrix} \in \mathbb{F}_q^{n \times n}$

Proof.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ if } \boxed{a^2+b^2 = -1}$$

□

Outline

Leading terms of the cost bounds for matrix multiplication

Definition (Leading term of a cost bound for matrix multiplication)

$$\mathrm{MM}_\omega(n) = C_\omega n^\omega$$

denotes the leading term in the arithmetic cost of an algorithm multiplying two $n \times n$ matrices (in $\mathrm{MM}_\omega(n) + o(\mathrm{MM}_\omega(n))$).

Leading terms of the cost bounds for matrix multiplication

Definition (Leading term of a cost bound for matrix multiplication)

$$\mathrm{MM}_\omega(n) = C_\omega n^\omega$$

denotes the leading term in the arithmetic cost of an algorithm multiplying two $n \times n$ matrices (in $\mathrm{MM}_\omega(n) + o(\mathrm{MM}_\omega(n))$).

Example

Classical method	$\mathrm{MM}_3(n) = 2n^3$
Strassen's algorithm	$\mathrm{MM}_{\log_2 7}(n) = 7n^{\log_2 7}$ with $\log_2(7) \approx 2.807$
Strassen-Winograd algorihtm	$\mathrm{MM}_{\log_2 7}(n) = 6n^{\log_2 7}$ with $\log_2(7) \approx 2.807$
Strassen-Winograd with base case at a threshold	$\begin{cases} C(n) \leqslant 7C(\lceil n/2 \rceil) + 15\lceil n/2 \rceil^2 \\ C(k) = 2k^3 \text{ for } k \lessapprox 1\,000 \end{cases}$
⋮	
[LeGall 2014]	$\omega < 2.3728639$

Leading terms of the arithmetic cost bounds for $A \cdot A^T$

- Classical method: $\frac{1}{2}\mathrm{MM}_3(n) = n^3$
- Our algorithm:
  - $S(n) \leqslant \boxed{3} S(\lceil n/2 \rceil) + \boxed{2} MM_\omega(\lceil n/2 \rceil) + \left(7.5 + \left\{ \begin{array}{c} 0 \\ 2 \\ 4 \\ 6 \end{array} \right\}\right) \lceil n/2 \rceil^2$ or $S(k) = k^3$ for $k \lessapprox 2\,000$
  - $\frac{2}{2^\omega - 3}\,\mathrm{MM}_\omega(n)$

Leading terms of the arithmetic cost bounds for $A \cdot A^T$

- Classical method: $\frac{1}{2}\mathrm{MM}_3(n) = n^3$
- Our algorithm:
  - $S(n) \leqslant \boxed{3} S(\lceil n/2 \rceil) + \boxed{2} MM_\omega(\lceil n/2 \rceil) + \left(7.5 + \left\{ \begin{array}{c} 0 \\ 2 \\ 4 \\ 6 \end{array} \right\}\right) \lceil n/2 \rceil^2$ or $S(k) = k^3$ for $k \lessapprox 2\,000$
  - $\frac{2}{2^\omega - 3}\,\mathrm{MM}_\omega(n)$

Problem	Algorithm	$\omega = 3$
$A \cdot A^T \in \mathbb{F}^{n \times n}$	D & C	n^3
	here	$0.8n^3$

Leading terms of the arithmetic cost bounds for $A \cdot A^T$

- Classical method: $\frac{1}{2}\mathrm{MM}_3(n) = n^3$
- Our algorithm:
  - $S(n) \leqslant \boxed{3} S(\lceil n/2 \rceil) + \boxed{2} MM_\omega(\lceil n/2 \rceil) + \left(7.5 + \left\{ \begin{array}{c} 0 \\ 2 \\ 4 \\ 6 \end{array} \right\}\right) \lceil n/2 \rceil^2$ or $S(k) = k^3$ for $k \lessapprox 2\,000$
  - $\frac{2}{2^\omega - 3}\,\mathrm{MM}_\omega(n)$

Problem	Algorithm	$\omega = 3$	$\omega = \log_2(7)$
$A \cdot A^T \in \mathbb{F}^{n \times n}$	D & C	n^3	$\frac{2}{3}\,\mathrm{MM}_{\log_2(7)}(n)$
	here	$0.8n^3$	$\frac{1}{2}\,\mathrm{MM}_{\log_2(7)}(n)$

Leading terms of the arithmetic cost bounds for $A \cdot A^T$

- Classical method: $\frac{1}{2}\mathrm{MM}_3(n) = n^3$
- Our algorithm:
  - $S(n) \leqslant \boxed{3} S(\lceil n/2 \rceil) + \boxed{2} MM_\omega(\lceil n/2 \rceil) + \left(7.5 + \left\{ \begin{array}{c} 0 \\ 2 \\ 4 \\ 6 \end{array} \right\}\right) \lceil n/2 \rceil^2$ or $S(k) = k^3$ for $k \lessapprox 2\,000$
  - $\frac{2}{2^\omega - 3}\,\mathrm{MM}_\omega(n)$

Problem	Algorithm	$\omega = 3$	$\omega = \log_2(7)$	ω
$A \cdot A^T \in \mathbb{F}^{n \times n}$	D & C	n^3	$\frac{2}{3}\,\mathrm{MM}_{\log_2(7)}(n)$	$\frac{2}{2^\omega - 4}\,\mathrm{MM}_\omega(n)$
	here	$0.8n^3$	$\frac{1}{2}\,\mathrm{MM}_{\log_2(7)}(n)$	$\frac{2}{2^\omega - 3}\,\mathrm{MM}_\omega(n)$

Leading terms of the cost bounds over $\mathbb{C}$

Counting field ops over $\mathbb{R}$

Problem	Algorithm	$\omega = 3$	$\omega = \log_2(7)$	ω
$A \cdot B \in \mathbb{C}^{n\times n}$	naive	$8n^3$	$4\,\mathrm{MM}^{\mathbb{R}}_{\log_2(7)}(n)$	$4\,\mathrm{MM}^{\mathbb{R}}_{\omega}(n)$
$(U+iV)\cdot(W+iX)$	Karatsuba: 3M	$6n^3$	$3\,\mathrm{MM}^{\mathbb{R}}_{\log_2(7)}(n)$	$3\,\mathrm{MM}^{\mathbb{R}}_{\omega}(n)$

*

Leading terms of the cost bounds over $\mathbb{C}$

Counting field ops over $\mathbb{R}$

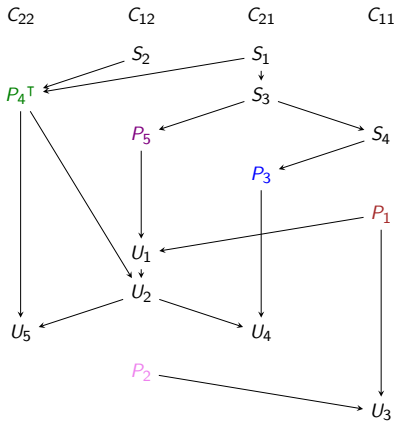
Problem	Algorithm	$\omega = 3$	$\omega = \log_2(7)$	ω
$A \cdot B \in \mathbb{C}^{n\times n}$	naive	$8n^3$	$4\,\mathrm{MM}^{\mathbb{R}}_{\log_2(7)}(n)$	$4\,\mathrm{MM}^{\mathbb{R}}_{\omega}(n)$
$(U+iV)\cdot(W+iX)$	Karatsuba: 3M	$6n^3$	$3\,\mathrm{MM}^{\mathbb{R}}_{\log_2(7)}(n)$	$3\,\mathrm{MM}^{\mathbb{R}}_{\omega}(n)$
$A \cdot A^{\mathsf{T}} \in \mathbb{C}^{n\times n}$	2M	$4n^3$	$2\,\mathrm{MM}^{\mathbb{R}}_{\log_2(7)}(n)$	$2\,\mathrm{MM}^{\mathbb{R}}_{\omega}(n)^{\star}$
	D & C	$3n^3$	$2\,\mathrm{MM}^{\mathbb{R}}_{\log_2(7)}(n)$	$\frac{6}{2^{\omega}-4}\,\mathrm{MM}^{\mathbb{R}}_{\omega}(n)$
	here	$2.4n^3$	$\frac{3}{2}\,\mathrm{MM}^{\mathbb{R}}_{\log_2(7)}(n)$	$\frac{6}{2^{\omega}-3}\,\mathrm{MM}^{\mathbb{R}}_{\omega}(n)$

*If $\omega < \log_2(6) \approx 2.585$, then $2 < \frac{6}{2^{\omega}-3}$

Outline

Scheduling

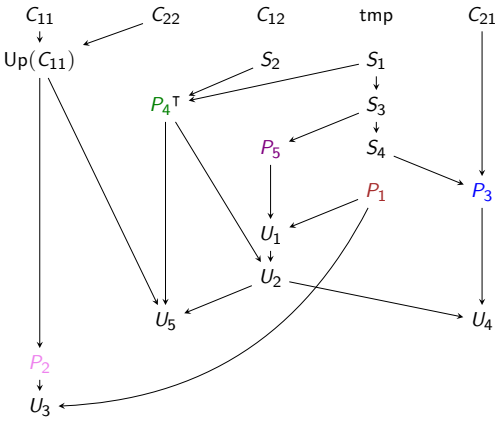
$$C \leftarrow \alpha A \cdot A^{\mathsf{T}}$$



#	operation	location
1	$S_1 = (A_{21} - A_{11}) \cdot Y$	C_{21}
2	$S_2 = A_{22} - A_{21} \cdot Y$	C_{12}
3	${P_4}^{\mathsf{T}} = S_2 \cdot {S_1}^{\mathsf{T}}$	C_{22}
4	$S_3 = S_1 - A_{22}$	C_{21}
5	$P_5 = S_3 \cdot {S_3}^{\mathsf{T}}$	C_{12}
6	$S_4 = S_3 + A_{12}$	C_{11}
7	$P_3 = A_{22} \cdot {S_4}^{\mathsf{T}}$	C_{21}
8	$P_1 = A_{11} \cdot {A_{11}}^{\mathsf{T}}$	C_{11}
9	$U_1 = P_1 + P_5$	C_{12}
	$\mathsf{Up}(U_1) = \mathsf{Low}(U_1)^{\mathsf{T}}$	C_{12}
10	$U_2 = U_1 + P_4$	C_{12}
11	$U_4 = U_2 + P_3$	C_{21}
12	$U_5 = U_2 + {P_4}^{\mathsf{T}}$	C_{22}
13	$P_2 = A_{12} \cdot {A_{12}}^{\mathsf{T}}$	C_{12}
14	$U_3 = P_1 + P_2$	C_{11}

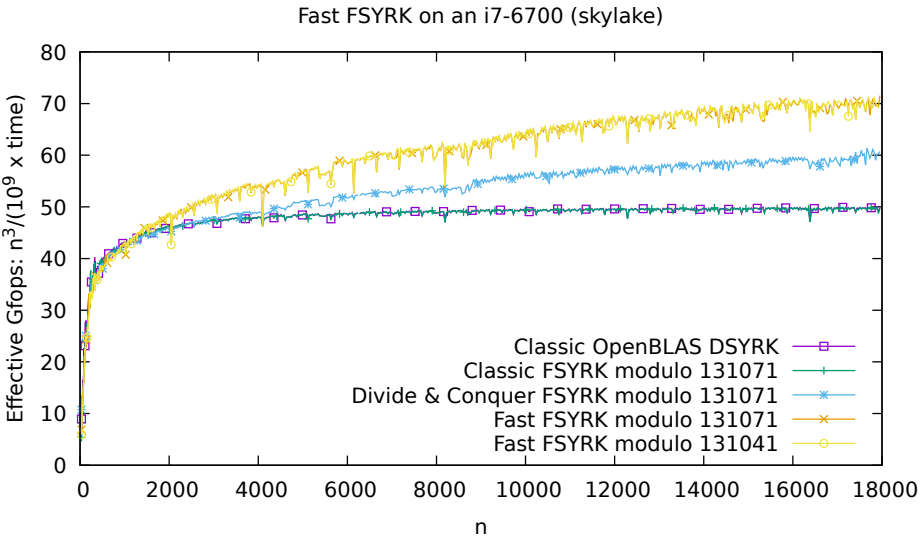
Scheduling

$C \leftarrow \alpha A \cdot A^{\mathsf{T}} + \beta C$ with one temporary block

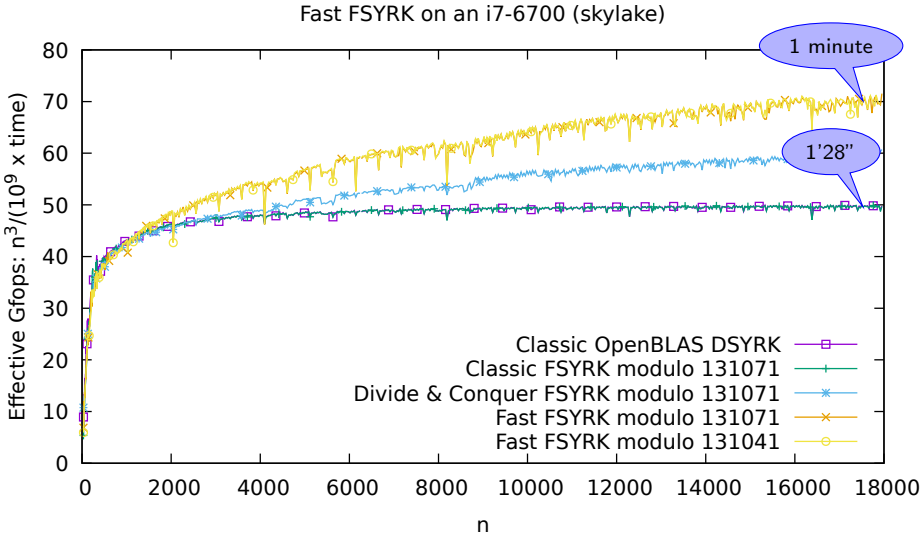


#	operation	location
1	$S_1 = (A_{21} - A_{11}) \cdot Y$	tmp $(\frac{n}{2} \times \frac{n}{2})$
2	$S_2 = A_{22} - A_{21} \cdot Y$	C_{12}
	$\mathrm{Up}(C_{11}) = \mathrm{Low}(C_{22})^{\mathsf{T}}$	C_{11}
3	$P_4{}^{\mathsf{T}} = \alpha S_2 \cdot S_1{}^{\mathsf{T}}$	C_{22}
4	$S_3 = S_1 - A_{22}$	tmp
5	$P_5 = \alpha S_3 \cdot S_3{}^{\mathsf{T}}$	C_{12}
6	$S_4 = S_3 + A_{12}$	tmp
7	$P_3 = \alpha A_{22} \cdot S_4{}^{\mathsf{T}} + \beta C_{21}$	C_{21}
8	$P_1 = \alpha A_{11} \cdot A_{11}{}^{\mathsf{T}}$	tmp
9	$U_1 = P_1 + P_5$	C_{12}
	$\mathrm{Up}(U_1) = \mathrm{Low}(U_1)^{\mathsf{T}}$	C_{12}
10	$U_2 = U_1 + P_4$	C_{12}
11	$U_4 = U_2 + P_3$	C_{21}
12	$U_5 = U_2 + P_4{}^{\mathsf{T}} + \beta \mathrm{Up}(C_{11})^{\mathsf{T}}$	C_{22}
13	$P_2 = \alpha A_{12} \cdot A_{12}{}^{\mathsf{T}} + \beta C_{11}$	C_{11}
14	$U_3 = P_1 + P_2$	C_{11}

Speed: LinBox/FFLAS-FFPACK



Speed: LinBox/FFLAS-FFPACK



Outline

On minimality of bilinear algorithms computing $A \cdot A^T$

Conjecture (5 multiplications)

1. 5 *multiplications required*
2. $5 = 3$ *recursive calls* $+2$ *general multiplications*

Conjecture (Skew orthogonal)

All variants with 5 *multiplications require a skew orthogonal matrix*

On minimality of bilinear algorithms computing $A \cdot A^T$

Conjecture (5 multiplications)

1. 5 *multiplications required*
2. $5 = 3$ *recursive calls* $+2$ *general multiplications*

Conjecture (Skew orthogonal)

All variants with 5 *multiplications require a skew orthogonal matrix*

Theorem (non-commutative)

Non-commutative 2×2 *variants with* 5 *multiplications require at least* 11 *additions*

Conjecture (9 additions)

All block variants with 5 *multiplications require at least* 9 *block additions*

On minimality of bilinear algorithms computing $A \cdot A^T$

Conjecture (5 multiplications)

1. 5 *multiplications required*
2. $5 = 3$ *recursive calls* $+2$ *general multiplications*

Conjecture (Skew orthogonal)

All variants with 5 *multiplications require a skew orthogonal matrix*

Theorem (non-commutative)

Non-commutative 2×2 *variants with* 5 *multiplications require at least* 11 *additions*

Conjecture (9 additions)

All block variants with 5 *multiplications require at least* 9 *block additions*

➡With symmetries of the blocks this is reduced to $\left(4+2+\frac{3}{2}\right)n^2 = 7.5n^2$ additions

Strassen tensor

Example: Winograd's variant

$$
\begin{aligned}
p_1 &= a_{11} \cdot b_{11} \\
p_2 &= a_{12} \cdot b_{21} \\
p_3 &= (a_{11} - a_{21}) \cdot (b_{22} - b_{12}) \\
p_4 &= (a_{21} + a_{22}) \cdot (b_{12} - b_{11}) \\
p_5 &= (a_{11} + a_{12} - a_{21} - a_{22}) \cdot b_{22} \\
p_6 &= a_{22}(b_{12} - b_{11} + b_{21} - b_{22}) \\
p_7 &= (a_{21} - a_{11} + a_{22}) \cdot (b_{11} - b_{12} + b_{22})
\end{aligned}
$$

$$
\begin{aligned}
c_{11} &= p_1 + p_2 \\
c_{12} &= p_1 + p_4 + p_5 + p_7 \\
c_{21} &= p_1 + p_3 + p_6 + p_7 \\
c_{22} &= p_1 + p_3 + p_4 + p_7
\end{aligned}
$$

$$
\begin{aligned}
\sum_{i=1}^{7} S_{i1} \otimes S_{i2} \otimes S_{i3} = {} & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \\
& \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + \\
& \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} -1 & 1 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \\
& \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}
\end{aligned}
$$

Strassen tensor

Example: Winograd's variant

$$
\begin{aligned}
p_1 &= a_{11} \cdot b_{11} \\
p_2 &= a_{12} \cdot b_{21} \\
p_3 &= (a_{11} - a_{21}) \cdot (b_{22} - b_{12}) \\
p_4 &= (a_{21} + a_{22}) \cdot (b_{12} - b_{11}) \\
p_5 &= (a_{11} + a_{12} - a_{21} - a_{22}) \cdot b_{22} \\
p_6 &= a_{22}(b_{12} - b_{11} + b_{21} - b_{22}) \\
p_7 &= (a_{21} - a_{11} + a_{22}) \cdot (b_{11} - b_{12} + b_{22})
\end{aligned}
$$

$$
\begin{aligned}
c_{11} &= p_1 + p_2 \\
c_{12} &= p_1 + p_4 + p_5 + p_7 \\
c_{21} &= p_1 + p_3 + p_6 + p_7 \\
c_{22} &= p_1 + p_3 + p_4 + p_7
\end{aligned}
$$

$$
\begin{aligned}
\sum_{i=1}^{7} S_{i1} \otimes S_{i2} \otimes S_{i3} = {} & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \\
& \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + \\
& \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} -1 & 1 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \\
& \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}
\end{aligned}
$$

Theorem (*[de Groot 1978]*)

All the 7 mult. variants $(U, V, W$ unimodular$)$ are given by:

$$\left(U^{-1} \cdot S_{i1} \cdot V\right) \otimes \left(V^{-1} \cdot S_{i2} \cdot W\right) \otimes \left(W^{-1} \cdot S_{i3} \cdot U\right)$$

Isotropy group and Gröbner basis: multiplications

5 multiplications for $A \cdot A^{\mathsf{T}}$?

- 12 **unknowns**: $U = \left[\begin{smallmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{smallmatrix}\right]$, $V = \left[\begin{smallmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{smallmatrix}\right]$, $W = \left[\begin{smallmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{smallmatrix}\right]$.
- 31 **equations of degree** 4
  - $3 * 4$ equations: recursive calls $p_i = X \cdot X^{\mathsf{T}}$ and
  - $2 * 2 * 4$ equations: two symmetries $p_j = X \cdot Y^{\mathsf{T}} = (Y \cdot X^{\mathsf{T}})^{\mathsf{T}} = p_k{}^{\mathsf{T}}$
  - 3 equations: unimodularity of U, V, W

Isotropy group and Gröbner basis: multiplications

5 multiplications for $A \cdot A^{\mathsf{T}}$?

Gröbner basis via FGb

$$\begin{cases} z &= v_{11} - v_{21} \\ v_{11} &= z + v_{21} \\ v_{22} &= \left(2\, v_{21}(v_{21}+z) - 1\right) v_{21} + z^3 \\ v_{12} &= -\left({v_{21}}^2 + \left(v_{21} + z^2\right)^2 + 1\right) v_{21} - z \\ u_{11} &= -\left(\left(z + v_{21}\right)^2 + {v_{21}}^2\right)(w_{21} + w_{22}) \\ u_{21} &= -\left(\left(z + v_{21}\right)^2 + {v_{21}}^2\right)(w_{11} + w_{12}) \\ u_{12} &= -\left(\left(z + v_{21}\right)^2 + {v_{21}}^2\right) w_{22} \\ u_{22} &= \left(\left(z + v_{21}\right)^2 + {v_{21}}^2\right) w_{12} \\ 1 &= w_{11} w_{22} - w_{12} w_{21} \\ 0 &= \left(\left(z + v_{21}\right)^2 + {v_{21}}^2\right)^2 + 1^\star \end{cases}$$

👍 $z^2 = \sqrt{-1}$, $v_{11} = 1$, $v_{21} = 0$, $w_{11} = 1$, $w_{12} = 0$, $w_{21} = 0$; then scale by $1/z$ ➡ our algorithm

---

$^\star 0 = \left(\left(z + v_{21}\right)^2 + {v_{21}}^2\right)^2 + 1$ imposes a square root of -1

Perspective

- Minimality of multiplications conjectures: reduce polynomial system?
  - ✓ 5 multiplications **are** required
  - ✓ except, 4 multiplications for: $(p{=}2)$ & $(2{\times}2)$ & (commutative)
  - ☺ conjectures verified $\forall$ isotropies of Strassen-Winograd ...

Perspective

- Minimality of multiplications conjectures: reduce polynomial system?
-  *[Schwartz et al. 2017, 2019]* for $A \cdot A^T$?
  - ☺ $O\left(n^2 \log(n)\right)$ non matrix based pre-computations ➡ only 12 additions
    - ☺ $\geqslant 5$ recursive levels: fewer operations than Strassen-Winograd for $A \cdot B$
    - ☹ Probably for matrices larger than $64k$ ...

Perspective

- Minimality of multiplications conjectures: reduce polynomial system?
-  *[Schwartz et al. 2017, 2019]* for $A \cdot A^{\mathsf{T}}$?
- Accelerating LDL^{T} in practice for arbitrary rank profile?