Matrix Multiplication

For a divide-and-conquer approach, we want an \( n \times n \) matrix to look like a matrix of smaller matrices:

\[
\begin{pmatrix}
  1 & 3 & 21 & 9 \\
  4 & 12 & 36 & 35 \\
  42 & 6 & 10 & 53 \\
  2 & 32 & 12 & 60 \\
\end{pmatrix}
\begin{pmatrix}
  41 & 2 & 6 & 14 \\
  3 & 11 & 7 & 18 \\
  40 & 13 & 16 & 29 \\
  7 & 19 & 63 & 72 \\
\end{pmatrix}
\]

How is a matrix of matrices like a matrix of integers?

Ring

\((S, +, \cdot, 0, 1)\)

Axioms

1. \(+, \cdot\) associate \((a+b)+c = a + (b+c)\)
2. \(+, \cdot\) commutes \(a+b = b+a\)
3. \(\cdot\) distributes over \(+\)
   \[a \cdot (a+c) = (a \cdot b) + (a \cdot c)\]
   \[(a+b) \cdot c = (a \cdot c) + (b \cdot c)\]
4. \(0\) is identity for \(+\) \(a+0 = 0+a = a\)
5. \(1\) is identity for \(\cdot\) \(a \cdot 1 = 1 \cdot a = a\)
6. every \(a\) in \(S\) has an additive inverse \(-a\)
   \(a + (-a) = 0\)
Example Ring

Integers modulo \( n \), \( \mathbb{Z}_n \)

- \([-a] \) is \([n-a]\)
- \(0\) is \([0]\)
- \(1\) is \([1]\)

\( \mathbb{Z}_4 \)

- \([-1] \) is \([4-1] = [3]\)
- \([1] + [3] = [4] = [0]\)

Key Example

\((M_n, +_n, \cdot_n, 0_n, 1_n)\)

\( n \times n \) matrices with elements from some ring \( R \)

Matrix add

Matrix multiplication

is a ring.

Inverse of \( A = (a_{ij}) \) is \( A^+ = (-a_{ij}) \)

Get weird

\( \mathbb{R}_{2, n/2} \) is \( 2 \times 2 \) matrices over the ring of \( \frac{n}{2} \times \frac{n}{2} \) matrices
Going Between $M_n$ and $R_{2, n/2}$

Let $A, B, C$ in $M_n$ where

$A', B', C' \in R_{2, n/2}$

$$\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$$

reduce $n \times n$ matrix mult to $n/2 \times n/2$ matrix ops

Complexity

Let $M(n)$ be the number of scalar operations in $R$ to multiply two $n \times n$ matrices over $R$

Divide-and-conquer doesn’t buy much

$$M(n) = 8 \cdot M\left(\frac{n}{2}\right) + \frac{n^2}{\log n} \leq 8 \cdot M\left(\frac{n}{2}\right) + n^2$$

In general, if

$$M(n) = m \cdot M\left(\frac{n}{2}\right) + a \cdot n^k$$

then $M(n) \leq kn^{\log m}$ for some $k$, provided $m > 4$
Complexity 2

If \( m = 8 \), as before
\[
M(n) = O(n^{\lg 8}) = O(n^3)
\]

If \( m = 7 \)
\[
M(n) = O(n^{\lg 7}) \geq O(n^{2.81})
\]

Need \( 2 \times 2 \) multiplication with 7 scalar multiplications
\[
\begin{pmatrix}
  a_{11} & a_{12} \\
  a_{21} & a_{22}
\end{pmatrix} \begin{pmatrix}
  b_{11} & b_{12} \\
  b_{21} & b_{22}
\end{pmatrix} = \begin{pmatrix}
  c_{11} & c_{12} \\
  c_{21} & c_{22}
\end{pmatrix}
\]

e.g., \( c_{22} = a_{21} \cdot b_{12} + a_{12} \cdot b_{22} \)

---

Strassen’s Algorithm

\[
\begin{align*}
  m_1 &= (a_{12} - a_{22}) \cdot (b_{21} + b_{22}) \\
  m_2 &= (a_{11} + a_{22}) \cdot (b_{11} + b_{22}) \\
  m_3 &= (a_{11} - a_{21}) \cdot (b_{11} + b_{12}) \\
  m_4 &= (a_{11} + a_{12}) \cdot b_{22} \\
  m_5 &= a_{11} \cdot (b_{12} - b_{22}) \\
  m_6 &= a_{22} \cdot (b_{21} - b_{11}) \\
  m_7 &= (a_{21} + a_{22}) \cdot b_{11}
\end{align*}
\]

Don’t want to use commutativity of multiplication
More Algebra

\[
c_{11} = m_1 + m_2 - m_4 + m_6
\]
\[
c_{12} = m_4 + m_5
\]
\[
c_{21} = m_6 + m_7
\]
\[
c_{22} = m_2 - m_3 + m_5 - m_7
\]
\[
= (a_{11}+a_{22})(b_{11}+b_{22}) - \frac{1}{16} a_{11} b_{12} - \frac{1}{16} a_{21} b_{12}
\]
\[
+ a_{11}(-b_{12}+b_{22}) - \frac{1}{16} a_{21} b_{11}
\]
\[
- (a_{21}+a_{22}) b_{11}
\]
\[
= a_{12} b_{21} + a_{11} b_{12} = a_{12} b_{21} + a_{11} b_{12}
\]
\[
= c_{22}
\]

Another Use of Matrix of Matrices

Connect matrix inversion with matrix multiplication

Inverse of matrix A, denoted A\(^{-1}\), is the unique matrix such that AA\(^{-1}\) = I

I is the identity matrix

Inverse doesn’t always exist

Example

\[
\begin{pmatrix}
1 & 2 \\
2 & 3
\end{pmatrix}
\begin{pmatrix}
-3 & 2 \\
2 & -1
\end{pmatrix}
= \begin{pmatrix}
-3+4 & 2-2 \\
-6+6 & 4-3
\end{pmatrix}
= \begin{pmatrix} 1 & 0 \\
0 & 1 \end{pmatrix}
\]

\[
A \\
A^{-1}
\]
Inversion vs. Multiplication

Assuming matrix inversion behaves reasonably, it has the same order as multiplication.

Let $I(n) =$ \# of scalar ops to invert an $n \times n$ matrix.
1. $I(n) \in \Omega(n^2)$
2. $I(3n) \in O(I(n))$

Time to multiply two $n \times n$ matrices, $M(n)$, is in $O(I(n))$.

Reduce Matrix Multiply to an Inversion Problem

Suppose we have $A, B$ to multiply, where both are $n \times n$.

Construct a $3n \times 3n$ matrix $D$

\[
\begin{pmatrix}
\text{In} & A & 0 \\
0 & \text{In} & B \\
0 & 0 & \text{In}
\end{pmatrix}
\]

Claim that $D^{-1}$ is

\[
\begin{pmatrix}
\text{In} & -A & AB \\
0 & \text{In} & -B \\
0 & 0 & \text{In}
\end{pmatrix}
\]
Check

$$DD^{-1} =$$

$$\begin{pmatrix}
\text{In} & A & 0 \\
0 & \text{In} & B \\
0 & 0 & \text{In}
\end{pmatrix}
\begin{pmatrix}
\text{In} & -A & AB \\
0 & \text{In} & -B \\
0 & 0 & \text{In}
\end{pmatrix} =$$

$$\begin{pmatrix}
\text{I} & \text{I} & -A + A & \text{I}A & -A & \text{B} \\
0 & \text{I} & \text{I} & -\text{I} & \text{B} + \text{B} & \text{I} \\
0 & 0 & \text{I} & \text{I}
\end{pmatrix}
\begin{pmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}$$