Matrix Multiplication (67826) – Exercise 2

Gal Cesana – 318510633

Question 1

We will demonstrate that the flip operation is not transitive using a simple example involving at most three multiplications.

Example

Consider the following three algorithms represented by trilinear terms:

$$\begin{aligned} A &: abc + xyz \\ B &: axc + byz \\ C &: xaz + byc \end{aligned}$$

Step-by-step analysis

1. **Flip from A to B:** A single flip is possible by swapping the variables b and x. The terms rearrange as:

$$abc + xyz \quad \to \quad axc + byz$$

2. **Flip from B to C:** Another single flip is possible by rearranging positions (a, x) and (c, z):

$$axc + byz \quad \to \quad xaz + byc$$

3. **Direct flip from A to C:** A direct single flip from A to C would require two independent simultaneous swaps ($a \leftrightarrow x$ and $c \leftrightarrow z$), which is not allowed by the definition of a single flip operation:

$$abc + xyz \qquad xaz + byc$$

Conclusion

This explicitly demonstrates that the flip operation is **not transitive**, since:

$$A \to B \text{ and } B \to C \text{ but } AC$$

Question 2

(a)

Strassen's algorithm over Z_2 in UVW representation (using modulo 2 arithmetic):

$$U = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad W = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

(b)

Using Hensel lifting from Z_2 to Z_4:

Given binary solution in Z_2: $a = b = d = 1$, $c = 0$ for equations:

$$ab + cd = 3$$
$$ad + cb = 1$$

Lift to Z_4:

$$ab + cd = (1)(1) + (0)(1) = 1 \equiv 3 \pmod 2$$
$$ad + cb = (1)(1) + (0)(1) = 1 \equiv 1 \pmod 2$$

Check mod 4: - For equation $ab + cd = 3$, we have $1 \not\equiv 3 \pmod 4$; thus, we add corrections:

$$a = 1 + 2\alpha, \quad b = 1 + 2\beta, \quad c = 0 + 2\gamma, \quad d = 1 + 2\delta$$

Checking mod 4:

$$(1 + 2\alpha)(1 + 2\beta) + (2\gamma)(1 + 2\delta) = 1 + 2(\alpha + \beta) \equiv 3 \pmod 4$$

This implies $2(\alpha + \beta) \equiv 2 \pmod 4$, thus $\alpha + \beta \equiv 1 \pmod 2$.

- For equation $ad + cb = 1$:

$$(1 + 2\alpha)(1 + 2\delta) + (2\gamma)(1 + 2\beta) = 1 + 2(\alpha + \delta) \equiv 1 \pmod 4$$

This implies $2(\alpha + \delta) \equiv 0 \pmod 4$, thus $\alpha + \delta \equiv 0 \pmod 2$.

Hence, possible lift solutions modulo 4 (choosing simplest solution):

$$\alpha = 0, \quad \beta = 1, \quad \gamma = 0, \quad \delta = 0$$

Therefore, a lifted solution modulo 4 is:

$$a = 1, \quad b = 3, \quad c = 0, \quad d = 1$$

Question 3

(a)

Translate the given trace representation into the UVW representation:
Given trace representation:

$$a_1b_1c_1 + a_1b_2c_2 + a_2b_2c_3$$

Expressed as UVW:

$$U = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad W = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Explanation: Each column in the matrices corresponds to one multiplication term from the trace representation, directly matching the given terms.

(b)

Translate Strassen's algorithm from UVW representation to a trace representation.

Given the UVW representation of Strassen's algorithm (as in previous exercises):

$$\langle U, V, W \rangle = \left\langle \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\rangle$$

The equivalent trace representation is:

$$\begin{aligned} \mathrm{Tr}(&(A_{11} + A_{22})(B_{11} + B_{22})C_{11} + (A_{21} + A_{22})B_{11}C_{21} \\ &+ A_{11}(B_{12} - B_{22})C_{12} + A_{22}(B_{21} - B_{11})C_{22} \\ &+ (A_{11} + A_{12})B_{22}C_{11} + (A_{21} - A_{11})(B_{11} + B_{12})C_{22} \\ &+ (A_{12} - A_{22})(B_{21} + B_{22})C_{11}) \end{aligned}$$

This matches exactly Strassen's well-known trace representation of the 2×2 matrix multiplication algorithm.

Question 4

(a)

The number of multiplications for the given algorithm as a function of n is:

$$\frac{(n+3)(n+2)(n+1)}{6} + \frac{105n^2}{16} + 39n + 55$$

(b)

For $n = 44$, the number of multiplications used is:

$$\frac{(44+3)(44+2)(44+1)}{6} + \frac{105 \times 44^2}{16} + 39 \times 44 + 55$$

Calculating explicitly:

$$\begin{aligned}
&= \frac{47 \times 46 \times 45}{6} + \frac{105 \times 1936}{16} + 1716 + 55 \\
&= 16215 + 12705 + 1771 \\
&= 30691
\end{aligned}$$

The exponent ω_0 is given by:

$$\omega_0 = \log_n(\text{number of multiplications}) = \log_{44}(30691) \approx 2.7275$$

Compared to known algorithms (e.g., Pan's algorithm with $\omega_0 \approx 2.773$), this is slightly better.

(c)

To find the optimal n divisible by four, we numerically optimize:

$$\omega_0 = \log_n\left(\frac{(n+3)(n+2)(n+1)}{6} + \frac{105n^2}{16} + 39n + 55\right)$$

Numerical optimization (e.g., using Desmos or computational tools) gives the optimal $n = 96$:

When $n = 96$:

$$\omega_0 = \log_{96}\left(\frac{(99)(98)(97)}{6} + \frac{105 \times 96^2}{16} + 39 \times 96 + 55\right) \approx 2.6959$$

Thus, the optimal exponent $\omega_0 \approx 2.6959$ at $n = 96$ is significantly better and demonstrates the importance of precise numerical optimization.