Grigoriev’s Lower Bound

**Theorem** Let \( f : A^n \to A^m \) be \((\alpha, n, m, p)\)-ind. and let it be realized by an SLP over the basis \( \Omega \). Every pebbling of every DAG for \( f \) requires space \( S \) and time \( T \) satisfying the inequality

\[
\lceil \alpha(S+1) \rceil T \geq mp/4
\]

**Theorem** The \( n \times n \) matrix multiplication function \( C = A \times B \) over ring \( R \) is \((1,2n^2,n^2,n)\)-independent.

**Corollary** The time \( T \) and space \( S \) required to realize the \( n \times n \) matrix multiplication function \( C = A \times B \) over a ring \( R \) using an SLP must satisfy

\[
(S+1)T \geq n^3/4
\]

Also, \( T \leq 2n^3 \) when \( S = 3 \).

**Proof** Do each inner product as shown below.

---

Grigoriev’s General Lower Bound

**Theorem** Let \( f : A^n \to A^m \) have a \( w(u,v) \)-flow & be realized by SLP with operators over \( A \). Let \( b \leq m \). Then every pebbling of SLP DAG requires space \( S \) and time \( T \) satisfying \( T \geq \lceil mb \rceil (n - d) \) where \( d \) is the largest integer such that \( w(d,b) \leq S \).
**Improved Matrix Multiplication Bounds**

**Lemma** Matrix multiplication has a \(w(u,v)\)-flow, satisfying
\[
w(u,v) \geq (v \cdot (2n^2 - u)^2) / 4n^2 / 2
\]

**Proof** Choose variables \(X_1\) from \(A\) and \(B\) and outputs \(Y_1\) from \(C\), \(|X_1| = u\). Let \(P(k)\) denote the \(n \times n\) permutation matrix that performs a left cyclic column permutation of a matrix by \(k\) positions, \(0 \leq k \leq n-1\).

Let \(A\) and \(B\) identify by 1’s the entries of \(A\) and \(B\) that are in \(X_1\). When \(A = P(k)\), let \(B(k) = P(k)B\). When \(B = P(k)\), let \(A(k) = AP(k)\). In the first case, \(B(k)\) is the downward cyclic shift of columns of \(A\) by \(k\) columns.

Let \(C\) be then \(n \times n\) matrix whose \((i,j)\) entry is 1 if \((i,j)\) entry of \(C\) is in \(Y_1\), \(|Y_1| = v\). If either \(A(k)\) and \(C\) or \(B(k)\) and \(C\) have many elements in common, matrix multiplication has large a flow.

---

**Improved Matrix Multiplication Bounds**

Let \(D\) and \(E\) be arbitrary square binary matrices.

Then, \(D \cap E\), the “intersection” of the two, is the binary matrix that contains 1’s only where both matrices contain 1’s.

Also, \(D \cup E\), the “union” of the two, is the binary matrix that contains 1’s where either \(D\) or \(E\) has 1’s.

The following hold.
\[
|D \cup E| + |D \cap E| = |D| + |E| \tag{1}
\]

Because \(|D \cup E| \leq n^2\) for \(n \times n\) matrices, we have
\[
|D \cap E| \geq |D| + |E| - n^2 \tag{2}
\]

Since \(|D \cap E| \geq 0\), we also have
\[
|D| + |E| \geq |D \cup E| \tag{3}
\]

**Note:** \(|A(r) \cap C| \mid (|B(s) \cap C|) = \text{number of elements in common between } A(r) \text{ and } C(B(r) \text{ and } C)\).

---

**Improved Matrix Multiplication Bounds**

If the max of \(|A(r) \cap C| \mid (|B(s) \cap C|)\) is large, there is a large \(w(u,v)\)-flow associated with matrix mult. But,
\[
\max(|A(r) \cap C|, |B(s) \cap C|) \geq Q(r,s)/2
\]

where
\[
Q(r,s) = |A(r) \cap C| + |B(s) \cap C|
\]

We show \(Q(r,s)\) is large for some \(r\) and \(s\). From (3)
\[
Q(r,s) \geq |C \cap (A(r) \cup B(s))|
\]

From (2) we have
\[
Q(r,s) \geq |Y_1| + |X_1| - n^2 - |A(r) \cap B(s)|
\]

Applying (1) we have
\[
Q(r,s) \geq |Y_1| + |A(r)| + |B(s)| - |A(r) \cap B(s)| - n^2
\]

where \(|C| = |Y_1|, |A(r)| = |A|, |B(s)| = |B|\). Since \(|X_1| = |A| + |B|\), we have
\[
Q(r,s) \geq |Y_1| + |X_1| - n^2 - |A(r) \cap B(s)|
\]

---

**Improved Matrix Multiplication Bounds**

Again
\[
Q(r,s) \geq |Y_1| + |X_1| - n^2 - |A(r) \cap B(s)|
\]

We show there exist \(r, s\) such that \(|A(r) \cap B(s)|\) is at most \(|A||B|/n^2\) which implies there are \(r, s\) such that
\[
Q(r,s) \geq |Y_1| + |X_1| - |A||B|/n^2 - n^2
\]

Here \(|X_1| - |A||B|/n^2\) is minimized by maximizing \(|A||B|\) subject to \(|X_1| = |A| + |B|\). Since \(|A||B| \leq (|X_1|/2)^2\)
\[
Q(r,s) \geq |Y_1| - n^2(1 - |X_1|^2/2n^2) = v - (2n^2 - u)^2/2n^2
\]

From
\[
\max(|A(r) \cap C|, |B(s) \cap C|) \geq Q(r,s)/2
\]

we have the desired result.

We now show that there exist \(r, s\) such \(|A(r) \cap B(s)|\) is at most \(|A||B|/n^2\).
**Improved Matrix Multiplication Bounds**

Let $S$ be

$$S = \sum_{r=1}^{n} \sum_{s=1}^{n} |A(r) \cap B(s)|$$

Since each 1 in $A$ is aligned with each 1 in $B$ by one of the cyclic shifts, $S = |A| |B|$. Since there must be some term that is at most equal to the average, we have

$$|A(r) \cap B(s)| \leq |A| |B|/n^2$$

from which the desired follows. ♥

---

**Improved Matrix Multiplication Bounds**

**Theorem** The $n \times n$ matrix multiplication (MM) function $C = A \times B$ over a ring $R$ satisfies

$$ST^2 \geq n^6/4$$

**Proof** We apply the generalized Grigoriev lower bound. Consider $b \leq m = n^2$. Then every pebbling of an SLP DAG for MM requires space $S$ and time $T$ satisfying $T \geq \lceil n^2/b \rceil (2n^2-d)$ where $d$ is the largest integer such that $w(d,b) \leq S$.

Since $w(u,v) \geq (v - (2n^2-u)^2/4n^2)/2$ let $b = 3S$. Then $w(d,b) \leq S$ when

$$(3S - (2n^2-d)^2/4n^2)/2 \leq S$$

This implies $(2n^2-d) \geq 2n\sqrt{S}$. Thus,

$$T \geq \lceil n^2/3S \rceil (2n^2-d) \geq 2n\sqrt{S} \lceil n^2/3S \rceil$$

$$\geq 2n\sqrt{S} (n^2 - 3S + 1)/3S$$

Now consider $S \leq n^2/27$ and $S \geq n^2/27$ with $T \geq 3n^2$ ♥