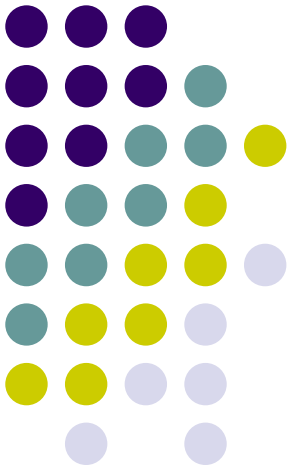
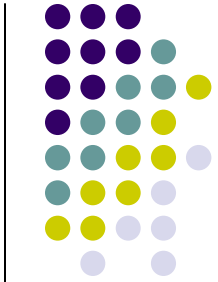
CS256
Applied Theory of Computation

Space-Time Tradeoffs III

John E Savage



Overview



- Improved space-time tradeoffs matrix multiplication

First Space-Time Tradeoff Inequality for Matrix Multiply

Corollary The time T and space S required to realize the $n \times n$ matrix multiplication function C = A × 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.

Grigoriev's General Lower Bound

Theorem Let $f : A^n \rightarrow A^m$ and let each output be dependent on each input. Let it have a $w(u,v)$-flow and 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 $T \geq \lfloor m/b \rfloor (n - d)$ 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

$$w(u,v) \geq (v - (2n^2-u)^2/4n^2)/2$$

Proof Choose variables X_1 from A and B and outputs Y_1 from C where $|X_1| = u$, $|Y_1| = v$. 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 $\mathcal{A}$ and $\mathcal{B}$ identify by 1's the entries of A and B that are in X_1. When A = P(k), let $\mathcal{B}(k) = P(k)\mathcal{B}$. When B = P($k$), let $\mathcal{A}(k) = \mathcal{A}P(k)$. In the first case, $\mathcal{B}(k)$ is the downward cylic shift of $\mathcal{B}$ by k rows. In the second, $\mathcal{A}(k)$ is the left cyclic shift of columns of $\mathcal{A}$ by k columns.

Let $\mathcal{C}$ be the $n \times n$ matrix whose (i,j) entry is 1 if (i,j) entry of C is in Y_1. If either $\mathcal{A}(k)$ and $\mathcal{C}$ or $\mathcal{B}(k)$ and $\mathcal{C}$ have many elements in common, ($|\mathcal{A}(r) \cap \mathcal{C}|$ or $|\mathcal{B}(s) \cap \mathcal{C}|$ is large) matrix multiplication has large a flow.

Improved Matrix Multiplication Bounds

Let $\mathcal{D}$ and $\mathcal{E}$ be arbitrary square binary matrices. Then, $\mathcal{D} \cap \mathcal{E}$, the "intersection" of the two, is the binary matrix that contains 1's only where both matrices contain 1's.

Also, $\mathcal{D} \cup \mathcal{E}$, the "union" of the two, is the binary matrix that contains 1's where either $\mathcal{D}$ or $\mathcal{E}$ has 1's.

$$|\mathcal{D} \cup \mathcal{E}| + |\mathcal{D} \cap \mathcal{E}| = |\mathcal{D}| + |\mathcal{E}| \qquad (1)$$

Because $|\mathcal{D} \cup \mathcal{E}| \leq n^2$ for $n \times n$ matrices, we have

$$|\mathcal{D} \cap \mathcal{E}| \geq |\mathcal{D}| + |\mathcal{E}| - n^2 \qquad (2)$$

Since $|\mathcal{D} \cap \mathcal{E}| \geq 0$, we also have

$$|\mathcal{D}| + |\mathcal{E}| \geq |\mathcal{D} \cup \mathcal{E}| \qquad (3)$$

Improved Matrix Multiplication Bounds

If the max of $|\mathcal{A}(r) \cap \mathcal{C}|$ or $|\mathcal{B}(s) \cap \mathcal{C}|$ is large, there is a large $w(u,v)$-flow associated with matrix mult. If

$$Q(r,s) = |\mathcal{A}(r) \cap \mathcal{C}| + |\mathcal{B}(s) \cap \mathcal{C}| \text{ then}$$

$$\textbf{max}\ (|\mathcal{A}(r) \cap \mathcal{C}|, |\mathcal{B}(s) \cap \mathcal{C}|) \geq Q(r,s)/2$$

We show $Q(r,s)$ is large for some r and s. From (3)

$$Q(r,s) \geq |C \cap (\mathcal{A}(r) \cup \mathcal{B}(s))|$$

From (2) we have

$$Q(r,s) \geq |C| + |\mathcal{A}(r) \cup \mathcal{B}(s)| - n^2$$

Improved Matrix Multiplication Bounds

Again,

$$Q(r,s) \geq |Y_1| + |X_1| - n^2 - |\mathcal{A}(r) \cap \mathcal{B}(s)|$$

We show there exist r, s such that $|\mathcal{A}(r) \cap \mathcal{B}(s)|$ is a most $|\mathcal{A}||\mathcal{B}|/n^2$ which implies there are r, s such that

$$Q(r,s) \geq |Y_1| + |X_1| - |\mathcal{A}||\mathcal{B}|/n^2 - n^2$$

Here $|X_1| - |\mathcal{A}||\mathcal{B}|/n^2$ is minimized by maximizing $|\mathcal{A}||\mathcal{B}|$ subject to $|X_1| = |\mathcal{A}| + |\mathcal{B}|$. Since $|\mathcal{A}||\mathcal{B}| \leq (|X_1|/2)^2$

$$Q(r,s) \geq |Y_1| - n^2(1 - |X_1|/2n^2)^2 = v - (2n^2-u)^2/2n^2$$

From

$$\mathbf{max}(|\mathcal{A}(r) \cap \mathcal{C}|, |\mathcal{B}(s) \cap \mathcal{C}|) \geq Q(r,s)/2$$

we have the desired result. We now show that there exist r, s such$|\mathcal{A}(r) \cap \mathcal{B}(s)|$ at most$|\mathcal{A}||\mathcal{B}|/n^2$.

Improved Matrix Multiplication Bounds

Let S be

$$S = \Sigma_{r = 1...n} \Sigma_{s = 1...n} |\mathcal{A}(r) \cap \mathcal{B}(s)|$$

Since each 1 in $\mathcal{A}$ is aligned with each 1 in $\mathcal{B}$ by one of the cyclic shifts, $S = |\mathcal{A}|\,|\mathcal{B}|$.

Because there must some term that is at most equal to the average, we have

$$|\mathcal{A}(r) \cap \mathcal{B}(s)| \leq |\mathcal{A}|\,|\mathcal{B}|/n^2$$

from which the desired result follows.♥

Improved Matrix Multiplication Bounds

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

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

- This is stronger than $(S+1)T \geq n^3/4$. To see this, assume that $ST^2 = n^6/4$ or $T = n^3/(2\sqrt{S})$. Then, $ST = \sqrt{S}\, n^3/2$ which is larger than $n^3/4$.

Improved Matrix Multiplication Bounds

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

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

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

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

$$T \ge \lfloor n^2/3S \rfloor (2n^2 - d) \ge 2n\sqrt{S} \lfloor n^2/3S \rfloor$$
$$\ge 2n\sqrt{S} (n^2 - 3S + 1)/3S$$

Now consider $S \le n^2/27$ and $S \ge n^2/27$ with $T \ge 3n^2$♥