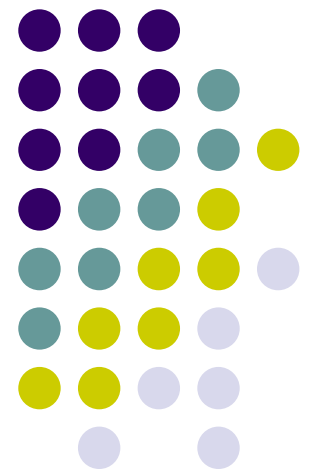


CS159 Introduction to Computational Complexity

Space-Time Tradeoffs II





The Problem

We study space-time tradeoffs for straight-line programs (SLPs) in which operations are over a basis $\Omega = \{h : A^r \rightarrow A^s \mid r, s \geq 1\}$.



Flow Properties of Functions

Definition Let X and Y be input and output variables of $f: A^n \rightarrow A^m$ and let $X_1 \subseteq X$ and $Y_1 \subseteq Y$. The subfunction $h = f|_{X_1}^{Y_1}$ maps inputs in X_1 to outputs in Y_1 by fixing $X - X_1$

f has a $w(u, v)$ -**flow** if for all $X_1 \subseteq X$ and $Y_1 \subseteq Y$, $|X_1| = u$ and $|Y_1| = v$, $h = f|_{X_1}^{Y_1}$ has at least $|A|^{w(u, v)}$ points in the image of its domain.



Flow Properties of Functions

Note: $w(u, v)$ is non-decreasing function of u and v .

$f: A^n \rightarrow A^m$ is (α, n, m, p) -**independent** for $\alpha \geq 1$ and $p \leq m$ if it has a $w(u, v)$ -flow satisfying $w(u, v) > (v/\alpha) - 1$ for $n - u + v \leq p$.

Note: Since $|X_1| = u$ and $|Y_1| = v$, $|X_0| + |Y_1| = n - u + v$.



Grigoriev's Lower Bound

Theorem Let $f : A^n \rightarrow A^m$ have a $w(u, v)$ -flow and be realized by SLP with operators over A in which each of output is dependent on the value of each input. Let $b \leq m$. Then every pebbling of SLP DAG requires space S and time T satisfying

$$T \geq \lfloor m/b \rfloor (n - d)$$

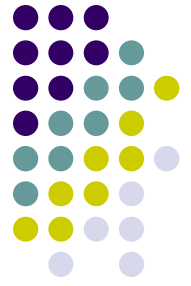
where d is the largest integer such that $w(d, b) \leq S$.



Grigoriev's Lower Bound

Proof Divide time steps into intervals during which b outputs are pebbled. Intervals begin with pebbling the first, $(b+1)$ st output, etc. The last interval has $m - b \lfloor m/b \rfloor$ outputs.

Let Y_1 be outputs pebbled in some specific interval. $|Y_1| = b$. Let X_0 and $X_1 = X - X_0$ be the inputs pebbled inside and before the interval. Let $x_0 = |X_0|$ and $x_1 = |X_1|$.

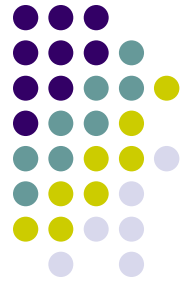


Grigoriev's Lower Bound

By definition there exists an assignment of values to inputs in X_0 so that outputs in Y_1 assume at least $|A|^y$ values, $y = w(x_1, b)$.

Since all variables in the interval (i.e. X_0) are fixed, the values of the outputs Y_1 are determined by inputs in X_1 .

Thus, if $w(x_1, b) > S$, outputs Y_1 assume more values than can be carried by $\leq S$ pebbles on a DAG at start of an interval, a contradiction.



Grigoriev's Lower Bound

Proof (cont.) Thus, $w(x_1, b) \leq S$. Since $w(u, v)$ is increasing in u and v , $x_1 \leq d$ where d is the largest integer satisfying $w(d, b) \leq S$. Because $x_0 + x_1 = n$, it follows that $x_0 \geq n - d$. Thus for each interval except possibly the last, $\geq n - d$ inputs are pebbled.

If T_1 is the number of steps on which inputs are pebbled,

$$T \geq T_1 \geq \lfloor m/b \rfloor (n - d)$$



Grigoriev's Lower Bound

Corollary Let $f : A^n \rightarrow A^m$ be (α, n, m, p) -ind. and let it be realized by an SLP over the basis W . Every pebbling of every DAG for f requires space S and time T satisfying the inequality

$$\lceil \alpha(S+1) \rceil T > mp/4$$



Grigoriev's Lower Bound

Proof An (α, n, m, p) -independent function on n inputs has a $w(u, v)$ -flow with $w(u, v) > (v/\alpha) - 1$ when $n - u + v \leq p$ where $x_0 = n - u \geq 0$.

The theorem requires $w(d, b) \leq S$ or $(b/\alpha) - 1 < S$ when $n - d + b \leq p$. Let $b = \lceil \alpha(S+1) \rceil$. Thus, $(b/\alpha) - 1 \geq S$. This implies that $(n - d) + b > p$ or $(n - d) > p - \lceil \alpha(S+1) \rceil$. Thus $T \geq \lfloor m/b \rfloor (n - d)$. Using $\lfloor m/x \rfloor \geq (m - x + 1)/x$, we have

$$T > (m - \lceil \alpha(S+1) \rceil + 1)(p - \lceil \alpha(S+1) \rceil) / \lceil \alpha(S+1) \rceil$$

Since $p \leq m$, if $\lceil \alpha(S+1) \rceil \leq p/2$, the result follows. If $\lceil \alpha(S+1) \rceil > p/2$, $\lceil \alpha(S+1) \rceil T > mp/2$, since $T \geq m$.

Flow Property of Matrix Multiplication



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

Proof Consider a set X_0 of inputs and a set Y_1 of outputs where $|X_0| + |Y_1| \leq n$. (Thus, $|X_0| \leq n$ and $|Y_1| \leq n$. Also, $|X_1| = |X| - |X_0| = 2n^2 - |X_0|$.)

Outputs in Y_1 fall into at most $|Y_1|$ columns of C . Inputs in X_0 fall into at most $|X_0|$ columns of A . Thus, at least $n - |X_0| = |Y_1|$ columns of A contain only variables.

Flow Property of Matrix Multiplication



Proof (cont.) Make B a permutation matrix that permutes the all-variables columns of A onto the at most $|Y_1|$ columns containing selected outputs. Because the variables in the all-variable columns of A are free to assume any values, the outputs in Y_1 , which are in $|Y_1|$ columns, can assume $|R|^y$ different values for $y = |Y_1|$. Thus, the function is $(1, 2n^2, n^2, n)$ -independent.

Flow Property of Matrix Multiplication



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

Corollary The time T and space S required to realize $n \times n$ matrix multiplication function C over R using an SLP must satisfy

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

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

