Checking Matrix Multiplication

A Randomized Algorithm

Mahmoud Ragab mahmoudr@uw.edu

CSEP 531 Spring 2016

Parallel Computation Computability and Complexity Theory

April 2016

Problem

- A, B, and C are matrices of size n x n.
- Question:

$$A \stackrel{?}{=} BC$$

$$A \stackrel{?}{=} BC$$

- Perform standard matrix multiplication for BxC and compare the results with A.
- O(n³) [n² output, each output requires n op]
- State of the art multiplication O(n^{2.373}) [Redefines the matrix to remove some redundant operations].
- Can we do better?

$$A \stackrel{?}{=} BC$$

- Choose a vector v = (v₁, v₂,, v_n) ∈ {-1, 1}
 n uniformly at random.
- Check Av = (BC)v.
- (BC)v = B(Cv) ← O(n²).
 [two matrix-vector multiplication]
- Pretty fast, but how accurate?

$$A \stackrel{?}{=} BC$$

Claim: If $A \neq BC$, then $P[Av = BCv] \leq \frac{1}{2}$

$$A \stackrel{?}{=} BC$$

- Proof: Let D = A BC
- Since A \square BC, then D \square 0.
- Let i, j be indices such that D_{ii} □ 0.
- Then:

$$A \stackrel{?}{=} BC$$

D = A - BC

$$\begin{bmatrix} D_{i0} & D_{i1} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \ddots & \vdots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & \dots & D_{ij} & \dots & \vdots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & D_{ij} & \dots & \dots \\ D_{in} & D_{in} & \dots & \dots \\ D_$$

$$P[Av = BCv] = P[Dv = 0] \le P[(Dv)i = 0]$$

$$(Dv)_i = \sum_{k=1}^n D_{ik} v_k$$
 $(Dv)_i = D_{ij} v_j + \sum_{k \neq j}^n D_{ik} v_k$

Questions?

