COMPSCI 690RA: Randomized Algorithms and Probabilistic Data Analysis

Prof. Cameron Musco

University of Massachusetts Amherst. Spring 2022.

Lecture 5

Logistics

- Project guidelines and suggested topics have been posted on the Assignments Tab of the course page.
- One page proposal due Monday 3/7.
- Problem Set 2 was posted last Friday – due next Thursday, 3/3. We will not have a quiz this week – focus on the problem set and project brainstorming instead.

Summary

Last Time: prime factorization

- Rabin fingerprint analysis. Applications to pattern matching (Rabin-Karp algorithm) and communication complexity (testing equality of n-bit strings using $O(\log n)$ bits).

m+n

- ℓ_0 sampling and low-communication graph connectivity.

Summary

Last Time:

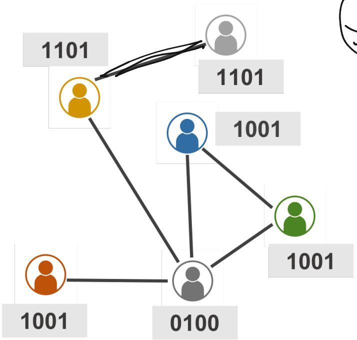
- Rabin fingerprint analysis. Applications to pattern matching (Rabin-Karp algorithm) and communication complexity (testing equality of n-bit strings using $O(\log n)$ bits).
- ℓ_0 sampling and low-communication graph connectivity.

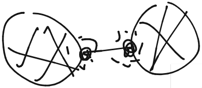
Today:

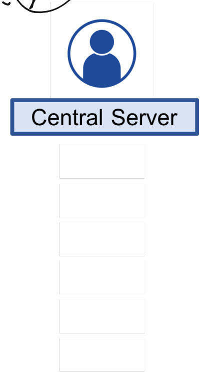
- Quickly finish up graph sketching and streaming.
- Start on randomized methods for linear algebraic computation.
- Approximate matrix multiplication via sampling.
- Stochastic trace estimation.

A Graph Communication Problem

Consider n nodes, each only knows its own neighborhood. They want to send messages to a central server, who must then determine if the graph is connected.

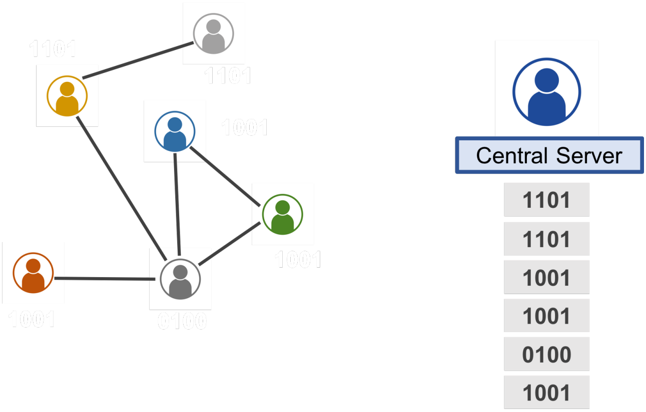






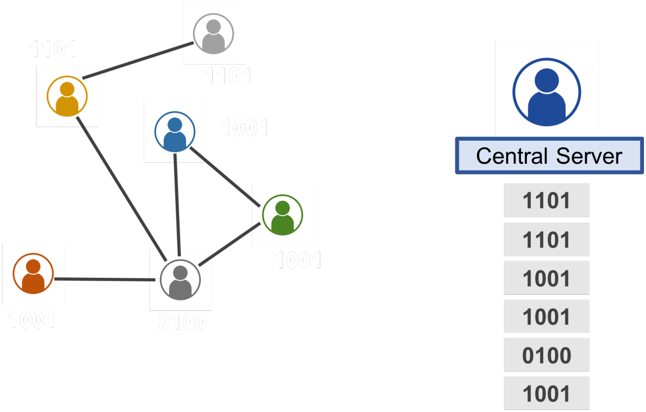
A Graph Communication Problem

Consider n nodes, each only knows its own neighborhood. They want to send messages to a central server, who must then determine if the graph is connected.



A Graph Communication Problem

Consider n nodes, each only knows its own neighborhood. They want to send messages to a central server, who must then determine if the graph is connected.



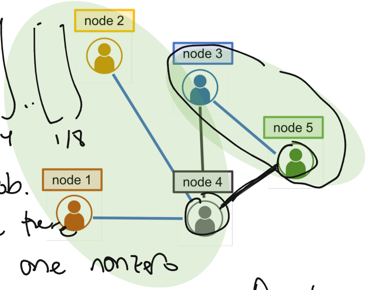
Saw how to solve the problem with high probability using just $O(\log^c n)$ sized messages.

- For independent ℓ_0 sampling matrices $\mathbf{A}_1, \ldots, \mathbf{A}_{\log_2 n}$, each node computes $\mathbf{A}_j v_i$ and sends these sketches to the central server. $O(\log^c n)$ bits in total.
- The central server uses $\mathbf{A}_j v_1, \ldots, \mathbf{A}_j v_n$ to simulate the j^{th} step of Boruvka's algorithm – the sketch allows the server to recover one outgoing edge from each connected component.

x

$1 \quad 1/2 \quad 1/4 \quad 1/8$

with good prob. at some rate there is exactly one nonzero entry remaining.



$\binom{n}{2}$

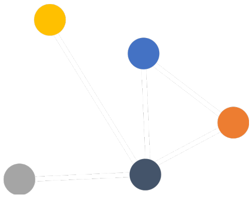
v_3		v_5			
0		0		0	(1,2)
0		0		0	(1,3)
0		0		0	(1,4)
0		0		0	(1,5)
0	+	0	=	0	(2,3)
0		0		0	(2,4)
0		0		0	(2,5)
1		0		1	(3,4)
1		-1		0	(3,5)
0		-1		-1	(4,5)

$A_j v_3 + A_j v_5 = A_j (v_3 + v_5)$

$a_j = \sum x_i \quad b_j = \sum i \cdot x_i \quad c_j = \sum r^i x_i \mod p$ where r is random

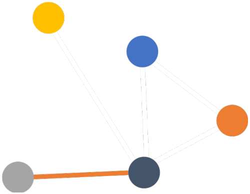
A Graph Streaming Problem

Consider a setting where an algorithm must process a stream of edge insertions or deletions, which define a graph. At the end of the stream, the algorithm should output whether that graph is connected or not.



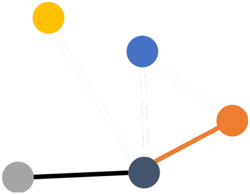
A Graph Streaming Problem

Consider a setting where an algorithm must process a stream of edge insertions or deletions, which define a graph. At the end of the stream, the algorithm should output whether that graph is connected or not.



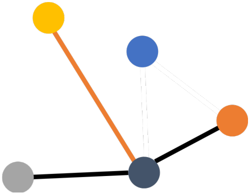
A Graph Streaming Problem

Consider a setting where an algorithm must process a stream of edge insertions or deletions, which define a graph. At the end of the stream, the algorithm should output whether that graph is connected or not.



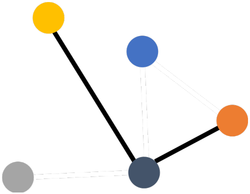
A Graph Streaming Problem

Consider a setting where an algorithm must process a stream of edge insertions or deletions, which define a graph. At the end of the stream, the algorithm should output whether that graph is connected or not.



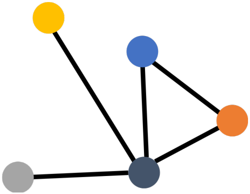
A Graph Streaming Problem

Consider a setting where an algorithm must process a stream of edge insertions or deletions, which define a graph. At the end of the stream, the algorithm should output whether that graph is connected or not.



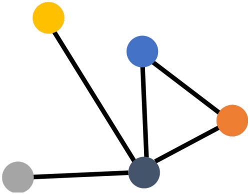
A Graph Streaming Problem

Consider a setting where an algorithm must process a stream of edge insertions or deletions, which define a graph. At the end of the stream, the algorithm should output whether that graph is connected or not.



A Graph Streaming Problem

Consider a setting where an algorithm must process a stream of edge insertions or deletions, which define a graph. At the end of the stream, the algorithm should output whether that graph is connected or not.

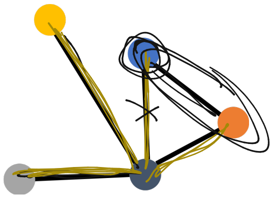


Algorithmic Question: How much memory must an algorithm use to solve this problem with high probability?

A Graph Streaming Problem

Consider a setting where an algorithm must process a stream of edge insertions or deletions, which define a graph. At the end of the stream, the algorithm should output whether that graph is connected or not.

n nodes



Algorithmic Question: How much memory must an algorithm use to solve this problem with high probability?

$O(n^2)$

What is the worst-case memory required by a naive deterministic algorithm that just stores the current state of the graph? How can you improve on this when there are no edge deletions?

Disjoint ($O(n \log n)$ space if only have insertions

Solution via ℓ_0 sampling

- The algorithm samples independent ℓ_0 sampling matrices $A_1, \ldots, A_{\log_2 n}$ and maintains $A_j v_u$ for all j and all $u \in [n]$, where $v_u \in \mathbb{R}^{\binom{n}{2}}$ is the incidence vector for node u.
- $O(n \log^c n)$ bits of storage in total.

$A_j v_u$ for all $j \in [1, .. \log_2 n]$
all $u \in [1, \ldots n]$

v_u

$\binom{n}{2}$

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}$$

Solution via ℓ_0 sampling

- The algorithm samples independent ℓ_0 sampling matrices $\mathsf{A}_1, \ldots, \mathsf{A}_{\log_2 n}$ and maintains $\mathsf{A}_j v_u$ for all j and all $u \in [n]$, where $v_u \in \mathbb{R}^{\binom{n}{2}}$ is the incidence vector for node u.
- $O(n \log^c n)$ bits of storage in total.
- When an edge (u, v) is inserted or deleted, one entry is either incremented or decremented in each of v_u, v_v. The algorithm can update $\mathsf{A}_j v_u$ and $\mathsf{A}_j v_v$ in $O(\log^c n)$ time – simply set $\mathsf{A}_j v_u = \mathsf{A}_j v_u \pm \mathsf{A}_{j,k}$.

Solution via ℓ_0 sampling

- The algorithm samples independent ℓ_0 sampling matrices $\mathsf{A}_1, \ldots, \mathsf{A}_{\log_2 n}$ and maintains $\mathsf{A}_j v_u$ for all j and all $u \in [n]$, where $v_u \in \mathbb{R}^{\binom{n}{2}}$ is the incidence vector for node u.
- $O(n \log^c n)$ bits of storage in total.
- When an edge (u, v) is inserted or deleted, one entry is either incremented or decremented in each of v_u, v_v. The algorithm can update $\mathsf{A}_j v_u$ and $\mathsf{A}_j v_v$ in $O(\log^c n)$ time – simply set $\mathsf{A}_j v_u = \mathsf{A}_j v_u \pm \mathsf{A}_{j,k}$.

$\binom{n}{2}$

$$\underbrace{\begin{bmatrix} 1 & -1 & 0 & 0 & 1 & -1 & 0 & 1 \\ -1 & 0 & 1 & 1 & 0 & 0 & -1 & 0 \\ 1 & 1 & -1 & 0 & -1 & -1 & 0 & 1 \\ 0 & -1 & -1 & -1 & 1 & 1 & 1 & 0 \end{bmatrix}}_{l_0 \text{ sampling matrix } \mathbf{A_j}} \underbrace{\begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}}_{v_u} = \underbrace{\begin{bmatrix} 1 \\ -2 \\ 1 \\ 1 \end{bmatrix}}_{\mathbf{A_j} v_u}$$

Solution via ℓ_0 sampling

- The algorithm samples independent ℓ_0 sampling matrices $\mathsf{A}_1, \ldots, \mathsf{A}_{\log_2 n}$ and maintains $\mathsf{A}_j v_u$ for all j and all $u \in [n]$, where $v_u \in \mathbb{R}^{\binom{n}{2}}$ is the incidence vector for node u.
- $O(n \log^c n)$ bits of storage in total.
- When an edge (u, v) is inserted or deleted, one entry is either incremented or decremented in each of v_u, v_v. The algorithm can update $\mathsf{A}_j v_u$ and $\mathsf{A}_j v_v$ in $O(\log^c n)$ time – simply set $\mathsf{A}_j v_u = \mathsf{A}_j v_u \pm \mathsf{A}_{j,k}$.

l_0 sampling matrix $\mathbf{A}_j$ $A_{j,k}$

$$\begin{bmatrix} 1 & -1 & 0 & 0 & 1 & -1 & 0 & 1 \\ -1 & 0 & 1 & 1 & 0 & 0 & -1 & 0 \\ 1 & 1 & -1 & 0 & -1 & -1 & 0 & 1 \\ 0 & -1 & -1 & -1 & 1 & 1 & 1 & 0 \end{bmatrix} \begin{array}{c} \mathrm{v_u} \\ \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \end{array} = \begin{array}{c} \mathbf{A_j}\mathrm{v_u} \\ \begin{bmatrix} 1 \\ -2 \\ 1 \\ 1 \end{bmatrix} \end{array}$$

$v_u(k)$

Solution via ℓ_0 sampling

- The algorithm samples independent ℓ_0 sampling matrices $\mathbf{A}_1, \ldots, \mathbf{A}_{\log_2 n}$ and maintains $\mathbf{A}_j v_u$ for all j and all $u \in [n]$, where $v_u \in \mathbb{R}^{\binom{n}{2}}$ is the incidence vector for node u.

post Nisan PRG

- $O(n \log^c n)$ bits of storage in total.
- When an edge (u, v) is inserted or deleted, one entry is either incremented or decremented in each of v_u, v_v. The algorithm can update $\mathbf{A}_j v_u$ and $\mathbf{A}_j v_v$ in $O(\log^c n)$ time – simply set $\mathbf{A}_j v_u = \mathbf{A}_j v_u \pm \mathbf{A}_{j,k}$.

Generate A:

$\binom{n}{2}$

l_0 sampling matrix $\mathbf{A}_j$ | v_u | $\mathbf{A}_j v_u$

$$\underbrace{\begin{bmatrix} 1 & -1 & 0 & 0 & 1 & -1 & 0 & 1 \\ -1 & 0 & 1 & 1 & 0 & 0 & -1 & 0 \\ 1 & 1 & -1 & 0 & -1 & -1 & 0 & 1 \\ 0 & -1 & -1 & -1 & 1 & 1 & 1 & 0 \end{bmatrix}}_{A_1, \ldots, A_j} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ -3 \\ 1 \\ 2 \end{bmatrix}$$

h(x) is 2-universal if for any $x \neq y$ $Pr[h(x) = h(y)] \leq \frac{1}{n}$ where n is the # outputs

$O(\log^c n)$

$[0, \ldots, p]$ seed random prime $< [0 \ldots p]$

Option 1: Build a from sufficiently random hash functions

Option 2: Use a PRG for space bounded computation to generate A.

Solution via ℓ_0 sampling

- The algorithm samples independent ℓ_0 sampling matrices $\mathsf{A}_1, \ldots, \mathsf{A}_{\log_2 n}$ and maintains $\mathsf{A}_j v_u$ for all j and all $u \in [n]$, where $v_u \in \mathbb{R}^{\binom{n}{2}}$ is the incidence vector for node u.
- $O(n \log^c n)$ bits of storage in total.
- When an edge (u, v) is inserted or deleted, one entry is either incremented or decremented in each of v_u, v_v. The algorithm can update $\mathsf{A}_j v_u$ and $\mathsf{A}_j v_v$ in $O(\log^c n)$ time – simply set $\mathsf{A}_j v_u = \mathsf{A}_j v_u \pm \mathsf{A}_{j,k}$.
- At the end of the stream (or at any time during it) can use the sketched neighborhoods to simulate Boruvka's algorithm and determine connectivity with high probability.

Solution via ℓ_0 sampling

- The algorithm samples independent ℓ_0 sampling matrices $\mathbf{A}_1, \ldots, \mathbf{A}_{\log_2 n}$ and maintains $\mathbf{A}_j v_u$ for all j and all $u \in [n]$, where $v_u \in \mathbb{R}^{\binom{n}{2}}$ is the incidence vector for node u.
- $O(n \log^c n)$ bits of storage in total.
- When an edge (u, v) is inserted or deleted, one entry is either incremented or decremented in each of v_u, v_v. The algorithm can update $\mathbf{A}_j v_u$ and $\mathbf{A}_j v_v$ in $O(\log^c n)$ time – simply set $\mathbf{A}_j v_u = \mathbf{A}_j v_u \pm \mathbf{A}_{j,k}$.
- At the end of the stream (or at any time during it) can use the sketched neighborhoods to simulate Boruvka's algorithm and determine connectivity with high probability.
- Can think of the algorithm as computing $\mathbf{AB} \in \mathbb{R}^{\log^3 n \times n}$ where $\underline{\mathbf{A} \in \mathbb{R}^{\log^3 n \times \binom{n}{2}}}$ is made up of the appended sketching matrices and $\underline{\mathbf{B} \in \mathbb{R}^{\binom{n}{2} \times n}}$ is the vertex-edge-incidence matrix.

$$A = \begin{bmatrix} A_1 \\ \hline A_2 \\ \hline \vdots \\ A_{\log n} \end{bmatrix}$$

$$[\,A\,][B] \overset{?}{=} [AB]$$

Approximate Matrix Multiplication

Matrix Multiplication Problem

n^3

Given $A, B \in \mathbb{R}^{n \times n}$ would like to compute $C = AB$. Requires $\underline{n^\omega}$ time where $\omega \approx 2.373$ in theory.

Matrix Multiplication Problem

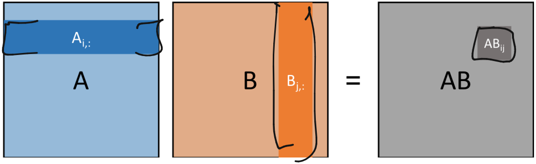
Given $A, B \in \mathbb{R}^{n \times n}$ would like to compute $C = AB$. Requires n^ω time where $\omega \approx 2.373$ in theory.

Today: We'll see how to compute an approximation in $O(n^2)$ time via a simple sampling approach.

- One of the most fundamental algorithms in randomized numerical linear algebra. Forms the building block for many other algorithms.

Outer Product View of Matrix Multiplication

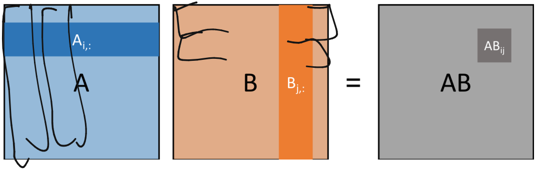
Inner Product View: $[AB]_{ij} = \langle A_{i,:}, B_{j,:} \rangle = \sum_{k=1}^{n} A_{ik} \cdot B_{kj}$.



n^2 inner products each takes n time $O(n^3)$

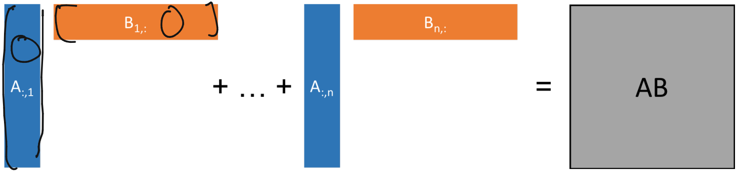
Outer Product View of Matrix Multiplication

Inner Product View: $[AB]_{ij} = \langle A_{i,:}, B_{j,:} \rangle = \sum_{k=1}^{n} A_{ik} \cdot B_{kj}$.



Outer Product View: Observe that $C_k = A_{:,k} B_{k,:}$ is an $n \times n$ matrix with $[C_k]_{ij} = A_{ik} \cdot B_{kj}$. So $AB = \sum_{k=1}^{n} A_{:,k} B_{k,:}$

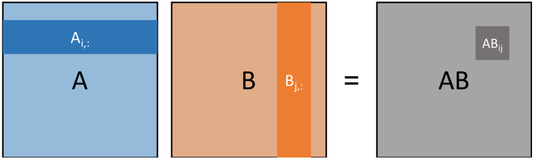
$[AB]_{ji} = \sum_{k=1} [C_k]_{ij} = \sum_{k=1} A_{ik} B_{kj}$
$= [AB]_{ji}$



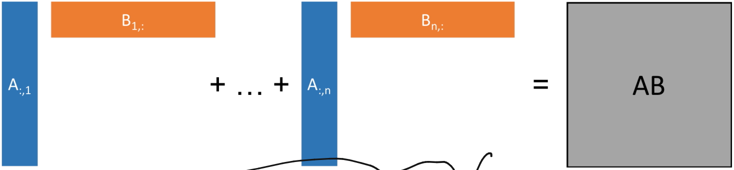
n outer product, each takes $O(n^2)$ time to compute → $O(n^3)$ time in total.

Outer Product View of Matrix Multiplication

Inner Product View: $[AB]_{ij} = \langle A_{i,:}, B_{j,:} \rangle = \sum_{k=1}^{n} A_{ik} \cdot B_{kj}$.



Outer Product View: Observe that $C_k = A_{:,k} B_{k,:}$ is an $n \times n$ matrix with $[C_k]_{ij} = A_{jk} \cdot B_{kj}$. So $AB = \sum_{k=1}^{n} A_{:,k} B_{k,:}$



n outer products

Basic Idea: Approximate **AB** by sampling terms of this sum.

Canonical AMM Algorithm

Approximate Matrix Multiplication (AMM): $\bar{C} \simeq AB = C$

- Fix sampling probabilities $p_1, \ldots, p_n$ with $p_i \geq 0$ and $\sum_{[n]} p_i = 1$.
- Select $\mathsf{i_1}, \ldots, \mathsf{i_t} \in [n]$ independently, according to the distribution $\Pr[\mathsf{i_j} = k] = p_k$.
- Let $\bar{\mathsf{C}} = \frac{1}{t} \cdot \sum_{j=1}^{t} \frac{1}{p_{\mathsf{i_j}}} \cdot A_{:,\mathsf{i_j}} B_{\mathsf{i_j},:}$.

Canonical AMM Algorithm

Approximate Matrix Multiplication (AMM):

- Fix sampling probabilities $p_1, \ldots, p_n$ with $p_i \geq 0$ and $\sum_{[n]} p_i = 1$.
- Select $\mathsf{i}_1, \ldots, \mathsf{i}_t \in [n]$ independently, according to the distribution $\Pr[\mathsf{i}_j = k] = p_k$.
- Let $\overline{\mathsf{C}} = \frac{1}{t} \cdot \sum_{j=1}^{t} \frac{1}{p_{\mathsf{i}_j}} \cdot A_{:,\mathsf{i}_j} B_{\mathsf{i}_j,:}$.

Claim 1: $\mathbb{E}[\overline{\mathsf{C}}] = AB$

Canonical AMM Algorithm

Approximate Matrix Multiplication (AMM):

- Fix sampling probabilities $p_1, \ldots, p_n$ with $p_i \geq 0$ and $\sum_{[n]} p_i = 1$.
- Select $\mathbf{i_1}, \ldots, \mathbf{i_t} \in [n]$ independently, according to the distribution $\Pr[\mathbf{i_j} = k] = p_k$.
- Let $\overline{\mathsf{C}} = \frac{1}{t} \cdot \sum_{j=1}^{t} \frac{1}{p_{\mathbf{i_j}}} \cdot A_{:,\mathbf{i_j}} B_{\mathbf{i_j},:}$.

Claim 1: $\mathbb{E}[\overline{\mathsf{C}}] = AB$

$$\mathbb{E}[\overline{\mathsf{C}}] = \frac{1}{t} \sum_{j=1}^{t} \mathbb{E}\left[\frac{1}{p_{\mathbf{i_j}}} \cdot A_{:,\mathbf{i_j}} B_{\mathbf{i_j},:}\right]$$

Approximate Matrix Multiplication (AMM):

- Fix sampling probabilities $p_1, \ldots, p_n$ with $p_i \geq 0$ and $\sum_{[n]} p_i = 1$.
- Select $\mathbf{i}_1, \ldots, \mathbf{i}_t \in [n]$ independently, according to the distribution $\Pr[\mathbf{i}_j = k] = p_k$.
- Let $\overline{\mathbf{C}} = \frac{1}{t} \cdot \sum_{j=1}^{t} \frac{1}{p_{\mathbf{i}_j}} \cdot A_{:,\mathbf{i}_j} B_{\mathbf{i}_j,:}$.

Claim 1: $\mathbb{E}[\overline{\mathbf{C}}] = AB$

index k with prob p_k

$$\mathbb{E}[\overline{\mathbf{C}}] = \frac{1}{t}\sum_{j=1}^{t} \underbrace{\mathbb{E}\left[\frac{1}{p_{\mathbf{i}_j}} \cdot A_{:,\mathbf{i}_j} B_{\mathbf{i}_j,:}\right]}_{} = \frac{1}{t}\sum_{j=1}^{t} \underbrace{\sum_{k=1}^{n} \cancel{p_k} \cdot \frac{1}{\cancel{p_k}} \cdot A_{:,k} B_{k,:}}_{\text{definition of expection}} = \frac{1}{t}\sum_{j=1}^{t} \underbrace{\sum_{k=1}^{n} A_{:k} \cdot B_{k:}}_{A \cdot B}$$

$$= \frac{1}{t}\sum_{j=1}^{t} A \cdot B = \underline{AB}$$

Canonical AMM Algorithm

Approximate Matrix Multiplication (AMM):

- Fix sampling probabilities $p_1, \ldots, p_n$ with $p_i \geq 0$ and $\sum_{[n]} p_i = 1$.
- Select $\mathsf{i}_1, \ldots, \mathsf{i}_\mathsf{t} \in [n]$ independently, according to the distribution $\Pr[\mathsf{i}_\mathsf{j} = k] = p_k$.
- Let $\overline{\mathsf{C}} = \frac{1}{t} \cdot \sum_{j=1}^{t} \frac{1}{p_{\mathsf{i}_\mathsf{j}}} \cdot A_{:,\mathsf{i}_\mathsf{j}} B_{\mathsf{i}_\mathsf{j},:}$.

Claim 1: $\mathbb{E}[\overline{\mathsf{C}}] = AB$

$$\mathbb{E}[\overline{\mathsf{C}}] = \frac{1}{t} \sum_{j=1}^{t} \mathbb{E}\left[\frac{1}{p_{\mathsf{i}_\mathsf{j}}} \cdot A_{:,\mathsf{i}_\mathsf{j}} B_{\mathsf{i}_\mathsf{j},:}\right] = \frac{1}{t} \sum_{j=1}^{t} \sum_{k=1}^{n} \cancel{p_k} \cdot \cancel{\frac{1}{p_k}} \cdot A_{:,k} B_{k,:} = \frac{1}{t} \underbrace{\sum_{j=1}^{t} AB}$$

Canonical AMM Algorithm

Approximate Matrix Multiplication (AMM):

- Fix sampling probabilities $p_1, \ldots, p_n$ with $p_i \geq 0$ and $\sum_{[n]} p_i = 1$.
- Select $\mathsf{i_1}, \ldots, \mathsf{i_t} \in [n]$ independently, according to the distribution $\Pr[\mathsf{i_j} = k] = p_k$.
- Let $\overline{\mathsf{C}} = \frac{1}{t} \cdot \sum_{j=1}^{t} \frac{1}{p_{\mathsf{i_j}}} \cdot A_{:,\mathsf{i_j}} B_{\mathsf{i_j},:}$.

Claim 1: $\mathbb{E}[\overline{\mathsf{C}}] = AB$

$$\mathbb{E}[\overline{\mathsf{C}}] = \frac{1}{t} \sum_{j=1}^{t} \mathbb{E}\left[\frac{1}{p_{\mathsf{i_j}}} \cdot A_{:,\mathsf{i_j}} B_{\mathsf{i_j},:}\right] = \frac{1}{t} \sum_{j=1}^{t} \sum_{k=1}^{n} p_k \cdot \frac{1}{p_k} \cdot A_{:,k} B_{k,:} = \frac{1}{t} \sum_{j=1}^{t} AB = AB$$

Canonical AMM Algorithm

Approximate Matrix Multiplication (AMM):

- Fix sampling probabilities $p_1, \ldots, p_n$ with $p_i \geq 0$ and $\sum_{[n]} p_i = 1$.
- Select $\mathbf{i_1}, \ldots, \mathbf{i_t} \in [n]$ independently, according to the distribution $\Pr[\mathbf{i_j} = k] = p_k$.
- Let $\bar{\mathbf{C}} = \frac{1}{t} \cdot \sum_{j=1}^{t} \frac{1}{p_{\mathbf{i_j}}} \cdot A_{:,\mathbf{i_j}} B_{\mathbf{i_j},:}$.

Claim 1: $\mathbb{E}[\bar{\mathbf{C}}] = AB$

$$\mathbb{E}[\bar{\mathbf{C}}] = \frac{1}{t} \sum_{j=1}^{t} \mathbb{E}\left[\frac{1}{p_{\mathbf{i_j}}} \cdot A_{:,\mathbf{i_j}} B_{\mathbf{i_j},:}\right] = \frac{1}{t} \sum_{j=1}^{t} \sum_{k=1}^{n} p_k \cdot \frac{1}{p_k} \cdot A_{:,k} B_{k,:} = \frac{1}{t} \sum_{j=1}^{t} AB = AB$$

Weighting by $\frac{1}{p_{\mathbf{i_j}}}$ keeps the expectation correct.

AMM Error Analysis

Claim 2: $\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

$\|M\|_F^2 = \sum m_{ij}^2$

AMM Error Analysis

Claim 2: $\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

$$\mathbb{E}[\|AB - \overline{C}\|_F^2] = \underbrace{\sum_{k,\ell} \mathbb{E}[([AB]_{k\ell} - \overline{C}_{k\ell})^2]}_{\text{def. of } \|\cdot\|_F^2 \text{ + linearity of expectation}}$$

def. of $\|\cdot\|_F^2$

+ linearity of expectation

AMM Error Analysis

Claim 2: $\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

$$\mathbb{E}[\|AB - \overline{C}\|_F^2] = \sum_{k,\ell} \mathbb{E}[([AB]_{k\ell} - \overline{C}_{k\ell})^2] = \sum_{k,\ell} \mathrm{Var}[\overline{C}_{k\ell}].$$

AMM Error Analysis

Claim 2: $\mathbb{E}[\|AB - \overline{\mathsf{C}}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

$$\mathbb{E}[\|AB - \overline{\mathsf{C}}\|_F^2] = \sum_{k,\ell} \mathbb{E}[([AB]_{k\ell} - \overline{\mathsf{C}}_{k\ell})^2] = \sum_{k,\ell} \mathrm{Var}[\overline{\mathsf{C}}_{k\ell}].$$

$$\mathrm{Var}[\overline{\mathsf{C}}_{k\ell}] = \mathrm{Var}\left[\frac{1}{t}\sum_{j=1}^{t} \frac{1}{p_{\mathrm{i_j}}} A_{k,\mathrm{i_j}} B_{\mathrm{i_j},\ell}\right]$$

$$\begin{bmatrix} A_{i_1} \\ 0 \end{bmatrix} \begin{bmatrix} B_{i_1} & 0 \end{bmatrix} + \begin{bmatrix} A_{i_2} \\ 0 \end{bmatrix} \begin{bmatrix} B_{i_2} & 0 \end{bmatrix} + \ldots$$

AMM Error Analysis

Claim 2: $\mathbb{E}[\|AB - \overline{\mathsf{C}}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

$$\mathbb{E}[\|AB - \overline{\mathsf{C}}\|_F^2] = \sum_{k,\ell} \mathbb{E}[([AB]_{k\ell} - \overline{\mathsf{C}}_{k\ell})^2] = \sum_{k,\ell} \mathrm{Var}[\overline{\mathsf{C}}_{k\ell}].$$

variance of 1 out of t trials

$$\mathrm{Var}[\overline{\mathsf{C}}_{k\ell}] = \mathrm{Var}\left[\frac{1}{t}\sum_{j=1}^{t} \frac{1}{p_{\mathrm{i_j}}} A_{k,\mathrm{i_j}} B_{\mathrm{i_j},\ell}\right] = \frac{1}{t}\,\underbrace{\mathrm{Var}\left[\frac{1}{p_{\mathrm{i_j}}} A_{k,\mathrm{i_j}} B_{\mathrm{i_j},\ell}\right]}$$

$\frac{1}{t^2}$

$$= \frac{1}{t^2} \mathrm{Var}\left[\sum_{j=1}^{t} \frac{1}{p_{i_j}} A_{k i_j} B_{i_j \ell}\right]$$

$$= \frac{1}{t^2} \cdot \sum_{j=1}^{t} \underbrace{\mathrm{Var}\left(\frac{1}{p_{i_j}} \cdots\right)}_{\sigma^2}$$

$$\frac{1}{t^2} \cdot \sum_{j=1}^{t} \sigma^2 = \frac{t}{t^2}\sigma^2 = \frac{1}{t} \cdot \sigma^2$$

AMM Error Analysis

Claim 2: $\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

$$\mathbb{E}[\|AB - \overline{C}\|_F^2] = \sum_{k,\ell} \mathbb{E}[([AB]_{k\ell} - \overline{C}_{k\ell})^2] = \sum_{k,\ell} \mathrm{Var}[\overline{C}_{k\ell}].$$

$\mathrm{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2$

$\leq \mathbb{E}[X^2]$

$$\mathrm{Var}[\overline{C}_{k\ell}] = \mathrm{Var}\left[\frac{1}{t}\sum_{j=1}^{t} \frac{1}{p_{i_j}} A_{k,i_j} B_{i_j,\ell}\right] = \frac{1}{t}\mathrm{Var}\left[\underbrace{\frac{1}{p_{i_j}} A_{k,i_j} B_{i_j,\ell}}_{\text{scalar}}\right]$$

$$\leq \frac{1}{t}\sum_{m=1}^{n} \underline{p_m} \cdot \frac{1}{\underline{p_m^2}} \cdot A_{k,m}^2 \cdot B_{m,\ell}^2$$

AMM Error Analysis

Claim 2: $\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

$$\mathbb{E}[\|AB - \overline{C}\|_F^2] = \sum_{k,\ell} \mathbb{E}[([AB]_{k\ell} - \overline{C}_{k\ell})^2] = \sum_{k,\ell} \mathrm{Var}[\overline{C}_{k\ell}].$$

$$\begin{aligned}
\mathrm{Var}[\overline{C}_{k\ell}] = \mathrm{Var}\left[\frac{1}{t}\sum_{j=1}^{t}\frac{1}{p_{i_j}}A_{k,i_j}B_{i_j,\ell}\right] &= \frac{1}{t}\mathrm{Var}\left[\frac{1}{p_{i_j}}A_{k,i_j}B_{i_j,\ell}\right] \\
&\leq \frac{1}{t}\sum_{m=1}^{n} p_m \cdot \frac{1}{p_m^2} \cdot A_{k,m}^2 \cdot B_{m,\ell}^2 \\
&= \frac{1}{t}\sum_{m=1}^{n} \frac{A_{k,m}^2 \cdot B_{m,\ell}^2}{p_m}
\end{aligned}$$

AMM Error Analysis

Claim 2: $\mathbb{E}[\|AB - \overline{\mathsf{C}}\|_F^2] \leqslant \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

$$\mathbb{E}[\|AB - \overline{\mathsf{C}}\|_F^2] = \sum_{k,\ell} \mathbb{E}[([AB]_{k\ell} - \overline{\mathsf{C}}_{k\ell})^2] = \sum_{k,\ell} \mathrm{Var}[\overline{\mathsf{C}}_{k\ell}].$$

$$\mathrm{Var}[\overline{\mathsf{C}}_{k\ell}] = \mathrm{Var}\left[\frac{1}{t}\sum_{j=1}^{t}\frac{1}{p_{\mathrm{i_j}}}A_{k,\mathrm{i_j}}B_{\mathrm{i_j},\ell}\right] = \frac{1}{t}\mathrm{Var}\left[\frac{1}{p_{\mathrm{i_j}}}A_{k,\mathrm{i_j}}B_{\mathrm{i_j},\ell}\right]$$

$$\leq \frac{1}{t}\sum_{m=1}^{n} p_m \cdot \frac{1}{p_m^2} \cdot A_{k,m}^2 \cdot B_{m,\ell}^2$$

$$= \frac{1}{t}\sum_{m=1}^{n} \frac{A_{k,m}^2 \cdot B_{m,\ell}^2}{p_m}$$

$$\mathbb{E}[\|AB - \overline{\mathsf{C}}\|_F^2] \leq \frac{1}{t} \cdot \sum_{m=1}^{n}\sum_{k=1}^{n}\sum_{\ell=1}^{n} \frac{A_{k,m}^2 \cdot B_{m,\ell}^2}{p_m}$$

$$\frac{1}{t} \cdot \sum_{m} \frac{1}{p_m} \sum_{k=1}^{n} A_{km}^2 \sum_{\ell=1} B_{m\ell}^2 - \|B_m\|_2^2$$

AMM Error Analysis

Claim 2: $\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

$$\mathbb{E}[\|AB - \overline{C}\|_F^2] = \sum_{k,\ell} \mathbb{E}[([AB]_{k\ell} - \overline{C}_{k\ell})^2] = \sum_{k,\ell} \mathrm{Var}[\overline{C}_{k\ell}].$$

$$\begin{aligned}
\mathrm{Var}[\overline{C}_{k\ell}] = \mathrm{Var}\left[\frac{1}{t}\sum_{j=1}^{t} \frac{1}{p_{\mathbf{i}_j}} A_{k,\mathbf{i}_j} B_{\mathbf{i}_j,\ell}\right] &= \frac{1}{t}\mathrm{Var}\left[\frac{1}{p_{\mathbf{i}_j}} A_{k,\mathbf{i}_j} B_{\mathbf{i}_j,\ell}\right] \\
&\leq \frac{1}{t}\sum_{m=1}^{n} p_m \cdot \frac{1}{p_m^2} \cdot A_{k,m}^2 \cdot B_{m,\ell}^2 \\
&= \frac{1}{t}\sum_{m=1}^{n} \frac{A_{k,m}^2 \cdot B_{m,\ell}^2}{p_m}
\end{aligned}$$

$$\mathbb{E}[\|AB - \overline{C}\|_F^2] \leq \frac{1}{t} \cdot \sum_{m=1}^{n}\sum_{k=1}^{n}\sum_{\ell=1}^{n} \frac{A_{k,m}^2 \cdot B_{m,\ell}^2}{p_m} = \underline{\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}}$$

Optimal Sampling Probabilities

Claim 2: $\mathbb{E}[\|AB - \bar{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

How should we set $p_1, \ldots, p_n$ to minimize this expected error?

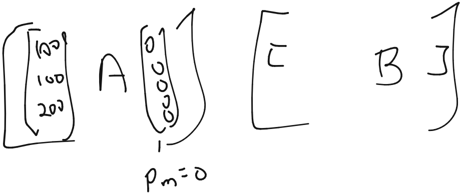
Claim 2: $\mathbb{E}[\|AB - \bar{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

How should we set $p_1, \ldots, p_n$ to minimize this expected error?

Set $p_m = \frac{\|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2}{\sum_{k=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2}$

$\sum_{m=1}^{n} p_m = 1$

(can derive e.g. using Lagrange multipliers. or Cauchy Schwarz.



Optimal Sampling Probabilities

Claim 2: $\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_{\cancel{2}}^{2} \cdot \|B_{m,:}\|_{\cancel{2}}^{2}}{p_m}$ $\|A_{:,m}\| \cdot \|B_{m,:}\|$

How should we set $p_1, \ldots, p_n$ to minimize this expected error?

Set $p_m = \frac{\|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2}{\sum_{k=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2}$, giving:

$$\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2 \cdot \left(\sum_{k=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2\right)$$

Optimal Sampling Probabilities

Claim 2: $\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

How should we set $p_1, \ldots, p_n$ to minimize this expected error?

Set $p_m = \frac{\|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2}{\sum_{k=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2}$, giving:

$$\mathbb{E}[\|AB - \overline{C}\|_F^2] \leq \frac{1}{t}\sum_{m=1}^{n} \|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2 \cdot \left(\sum_{k=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2\right)$$

$$= \frac{1}{t}\left(\sum_{m=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2\right)^2$$

Optimal Sampling Probabilities

Claim 2: $\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

How should we set $p_1, \ldots, p_n$ to minimize this expected error?

Set $p_m = \frac{\|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2}{\sum_{k=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2}$, giving:

$$\mathbb{E}[\|AB - \overline{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2 \cdot \left(\sum_{k=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2\right)$$

$$= \frac{1}{t}\left(\sum_{m=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2\right)^2$$

$$\langle x, y \rangle \leq \|x\|_2 \cdot \|y\|_2$$

By the Cauchy-Schwarz inequality,

$$\sum_{m=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2 \leq \sqrt{\sum_{m=1}^{n} \|A_{:,k}\|_2^2} \cdot \sqrt{\sum_{m=1}^{n} \|B_{k,:}\|_2^2} = \|A\|_F \cdot \|B\|_F$$

$$\begin{bmatrix} \|A_{:,1}\|_2 \\ \vdots \\ \|A_{:,n}\|_2 \end{bmatrix} \quad \begin{bmatrix} \|B_{1,:}\|_2 \\ \vdots \\ \|B_{n,:}\|_2 \end{bmatrix}$$

Optimal Sampling Probabilities

Claim 2: $\mathbb{E}[\|AB - \bar{C}\|_F^2] = \frac{1}{t}\sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.

How should we set $p_1, \ldots, p_n$ to minimize this expected error?

Set $p_m = \frac{\|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2}{\sum_{k=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2}$, giving:

$$\begin{aligned}
\mathbb{E}[\|AB - \bar{C}\|_F^2] &= \frac{1}{t}\sum_{m=1}^{n} \|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2 \cdot \left(\sum_{k=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2\right) \\
&= \frac{1}{t}\left(\sum_{m=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2\right)^2
\end{aligned}$$

By the Cauchy-Schwarz inequality,

$\sum_{m=1}^{n} \|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2 \leq \sqrt{\sum_{m=1}^{n} \|A_{:,k}\|_2^2} \cdot \sqrt{\sum_{m=1}^{n} \|B_{k,:}\|_2^2} = \|A\|_F \cdot \|B\|_F$

Overall: $\boxed{\mathbb{E}[\|AB - \bar{C}\|_F^2] \leq \frac{\|A\|_F^2 \cdot \|B\|_F^2}{t}}$ Setting $t = \frac{1}{\epsilon^2\sqrt{\delta}}$, by Chebyshev's inequality:

$$\Pr[\|AB - \bar{C}\|_F \geq \epsilon \cdot \|A\|_F \cdot \|B\|_F] \leq \delta.$$

AMM Upshot

Upshot: Sampling $t = O(1/\epsilon^2)$ columns/rows of A, B with probabilities proportional to $\|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2$ yields, with good probability, an approximation $\overline{\mathbf{C}}$ with

$$\|AB - \overline{\mathbf{C}}\|_F \leq \epsilon \cdot \|A\|_F \cdot \|B\|_F.$$

AMM Upshot

Upshot: Sampling $t = O(1/\epsilon^2)$ columns/rows of A, B with probabilities proportional to $\|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2$ yields, with good probability, an approximation $\overline{C}$ with

$$\|AB - \overline{C}\|_F \leq \epsilon \cdot \|A\|_F \cdot \|B\|_F.$$

- Probabilities take $O(n^2)$ time to compute. After sampling, $\overline{C}$ takes $O(t \cdot n^2)$ time to compute.

$O(n/\varepsilon^2)$ vs. $O(n^3)$

AMM Upshot

Upshot: Sampling $t = O(1/\epsilon^2)$ columns/rows of A, B with probabilities proportional to $\|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2$ yields, with good probability, an approximation $\overline{C}$ with

$$\|AB - \overline{C}\|_F \leq \epsilon \cdot \|A\|_F \cdot \|B\|_F.$$

- Probabilities take $O(n^2)$ time to compute. After sampling, $\overline{C}$ takes $O(t \cdot n^2)$ time to compute.
- Can derive related bounds when probabilities are just approximate – i.e. $p_k \geq \beta \cdot \frac{\|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2}{\sum_{m=1}^{n} \|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2}$ for some $\beta > 0$.

AMM Upshot

Upshot: Sampling $t = O(1/\epsilon^2)$ columns/rows of A, B with probabilities proportional to $\|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2$ yields, with good probability, an approximation $\overline{C}$ with

$$\|AB - \overline{C}\|_F \leq \epsilon \cdot \|A\|_F \cdot \|B\|_F.$$

- Probabilities take $O(n^2)$ time to compute. After sampling, $\overline{C}$ takes $O(t \cdot n^2)$ time to compute.
- Can derive related bounds when probabilities are just approximate – i.e. $p_k \geq \beta \cdot \frac{\|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2}{\sum_{m=1}^{n} \|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2}$ for some $\beta > 0$.
- Can also give bounds on $\|AB - \overline{C}\|_2$, but analysis is much more complex. Will see tools in the coming weeks that let us do this.

AMM Upshot

Upshot: Sampling $t = O(1/\epsilon^2)$ columns/rows of A, B with probabilities proportional to $\|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2$ yields, with good probability, an approximation $\bar{\mathbf{C}}$ with

$$\|AB - \bar{\mathbf{C}}\|_F \leq \epsilon \cdot \|A\|_F \cdot \|B\|_F.$$

- Probabilities take $O(n^2)$ time to compute. After sampling, $\bar{\mathbf{C}}$ takes $O(t \cdot n^2)$ time to compute.
- Can derive related bounds when probabilities are just approximate – i.e. $p_k \geq \beta \cdot \frac{\|A_{:,k}\|_2 \cdot \|B_{k,:}\|_2}{\sum_{m=1}^{n} \|A_{:,m}\|_2 \cdot \|B_{m,:}\|_2}$ for some $\beta > 0$.
- Can also give bounds on $\|AB - \bar{\mathbf{C}}\|_2$, but analysis is much more complex. Will see tools in the coming weeks that let us do this.
- A classic example of using weighted sampling to decrease variance and in turn, sample complexity.

AMM Upshot

$$\|AB - \bar{C}\|_F < \epsilon \cdot \|A\|_F \cdot \|B\|_F$$

Think-Pair-Share 1: Ideally we would have *relative error*, $\boxed{\|AB - \bar{C}\|_F \le \epsilon \|AB\|_F}$. Could we get this via a tighter analysis or better sampling distribution?

$$\|AB\|_F << \|A\|_F \cdot \|B\|_F$$

$$A = \begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & 0 & \\ & & & & & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & & & & & \\ & 0 & & & & \\ & & 0 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix}$$

$$\|A\|_F = \|B\|_F \approx \sqrt{n/2}$$

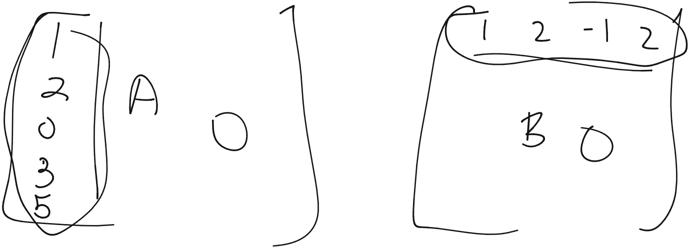
$$\|AB\|_F = 0$$

$$\begin{bmatrix} & A & \end{bmatrix} \cdot \begin{bmatrix} & B & \end{bmatrix} = \begin{bmatrix} & 0 & \end{bmatrix}$$

$$O(n^{2+c})$$

Think-Pair-Share 1: Ideally we would have *relative error*, $\|AB - \bar{C}\|_F \leq \epsilon \|AB\|_F$. Could we get this via a tighter analysis or better sampling distribution?

Think-Pair-Share 2: What if we just uniformly sampled rows/columns? Recall that $\mathbb{E}[\|AB - \bar{C}\|_F^2] = \frac{1}{t} \sum_{m=1}^{n} \frac{\|A_{:,m}\|_2^2 \cdot \|B_{m,:}\|_2^2}{p_m}$.



$$\|AB - \bar{C}\|_F = \|AB\|_F$$

Stochastic Trace Estimation

Matrix Trace

The trace of a matrix $A \in \mathbb{R}^{n \times n}$ is the sum of it diagonal entries.

$$\mathrm{tr}(A) = \sum_{i=1}^{n} A_{ii}.$$

When A is diagonalizable (e.g., when it is symmetric) with eigenvalues $\lambda_1, \ldots, \lambda_n$, $\mathrm{tr}(A) = \sum_{i=1}^{n} \lambda_i$.

Matrix Trace

The trace of a matrix $A \in \mathbb{R}^{n \times n}$ is the sum of it diagonal entries.

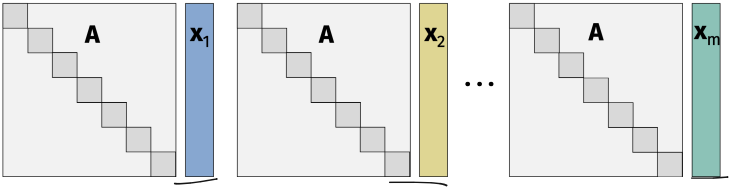
$$\mathrm{tr}(A) = \sum_{i=1}^{n} A_{ii}.$$

When A is diagonalizable (e.g., when it is symmetric) with eigenvalues $\lambda_1, \ldots, \lambda_n$, $\mathrm{tr}(A) = \sum_{i=1}^{n} \lambda_i$.

How many operations does it take to compute $\mathrm{tr}(A)$ given explicit access to A? n operations

Implicit Trace Estimation

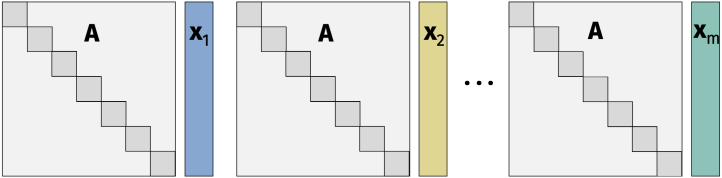
- Given implicit access to $A \in \mathbb{R}^{n \times n}$ through **matrix-vector multiplication**.
- Goal is to approximate $\text{tr}(A) = \sum_{i=1}^{n} A_{ii}$.



Main question: How many matrix-vector multiplication "queries" $Ax_1, \ldots, Ax_m$ are required to approximate $\text{tr}(A)$?

Implicit Trace Estimation

- Given implicit access to $A \in \mathbb{R}^{n\times n}$ through **matrix-vector multiplication**.
- Goal is to approximate $\mathrm{tr}(A) = \sum_{i=1}^{n} A_{ii}$.



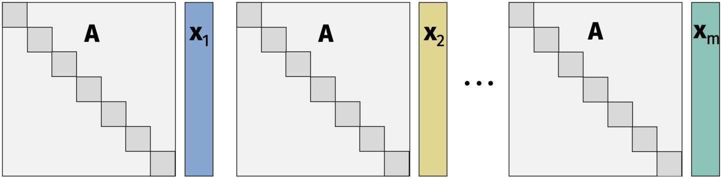
Main question: How many matrix-vector multiplication "queries" $Ax_1, \ldots, Ax_m$ are required to approximate $\mathrm{tr}(A)$?

Algorithms in this model are called matrix-free methods. Useful when A is not given explicitly, but we have an efficient algorithm for multiplying A by a vector (examples to come).

Implicit Trace Estimation

- Given implicit access to $A \in \mathbb{R}^{n \times n}$ through **matrix-vector multiplication**.
- Goal is to approximate $\operatorname{tr}(A) = \sum_{i=1}^{n} A_{ii}$.

$\log^2 n \; [\,A \; \binom{n}{2}\,] \; [\,B\,]$ n



Main question: How many matrix-vector multiplication "queries" $Ax_1, \ldots, Ax_m$ are required to approximate $\operatorname{tr}(A)$?

$(AB - C) = 0$

Algorithms in this model are called matrix-free methods. Useful when A is not given explicitly, but we have an efficient algorithm for multiplying A by a vector (examples to come).

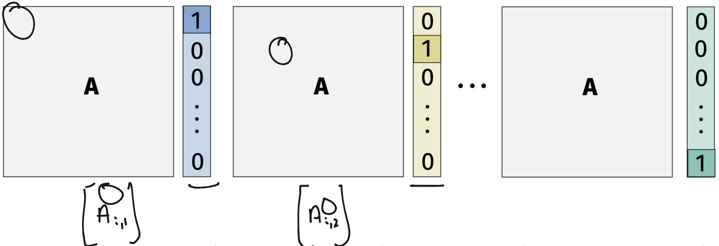
$(AB - C)x$

What other matrix free method have we studied in this class?

Naive Exact Algorithm

Naive solution:

- Set $x_i = e_i$ for $i = 1, \ldots, n$.
- Return $\mathrm{tr}(A) = \sum_{i=1}^{n} x_i^T A x_i$. $= A_{ii}$

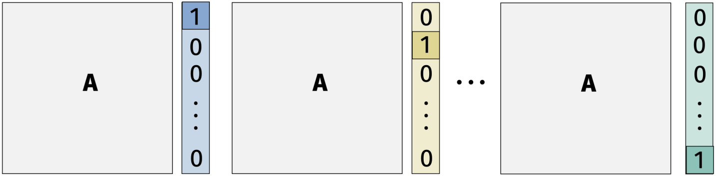


Returns exact solution, but requires n matrix-vector multiplies.

Naive Exact Algorithm

Naive solution:

- Set $x_i = e_i$ for $i = 1, \ldots, n$.
- Return $\mathrm{tr}(A) = \sum_{i=1}^{n} x_i^T A x_i$.

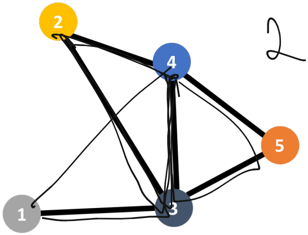


Returns exact solution, but requires n matrix-vector multiplies.

We will see how to use $m \ll n$ multiplies by using randomness and allowing for small approximation error.

Motivating Example

The number of triangles or other small 'motifs' is an important metric of network connectivity. E.g., important in computing the network clustering coefficient

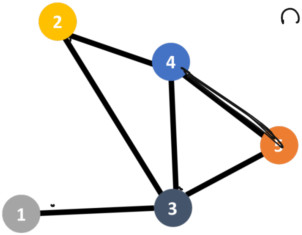


2 triangles

Motivating Example

The number of triangles or other small 'motifs' is an important metric of network connectivity. E.g., important in computing the network clustering coefficient

n node graph



How long does it take to exactly compute the number of triangles in the graph?

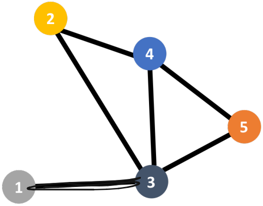
$|E| \cdot n$

$\binom{n}{3}$ triples to check

$O(n^3)$ runtime

Motivating Example

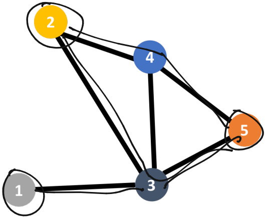
Can use the adjacency matrix $B \in \{0,1\}^{n \times n}$ to write the number of triangles in a linear algebraic way.



$$\mathbf{B} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Motivating Example

Can use the adjacency matrix $B \in \{0,1\}^{n \times n}$ to write the number of triangles in a linear algebraic way.

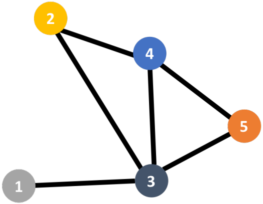


$$B = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

- B_{ij} indicates the number of 1-step paths (edges) from i, j
- $[B^2]_{ij}$ indicates the number of 2-step paths from i, j
- $[B^3]_{ij}$ indicates the number of 3-step paths from i, j

Motivating Example

Can use the adjacency matrix $B \in \{0,1\}^{n \times n}$ to write the number of triangles in a linear algebraic way.



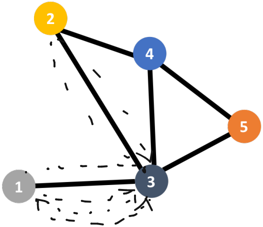
B²

1	1	0	1	1
1	2	1	1	2
0	1	4	2	1
1	1	2	3	1
1	2	1	1	2

- B_{ij} indicates the number of 1-step paths (edges) from i, j
- $[B^2]_{ij}$ indicates the number of 2-step paths from i, j
- $[B^3]_{ij}$ indicates the number of 3-step paths from i, j

Motivating Example

Can use the adjacency matrix $B \in \{0,1\}^{n \times n}$ to write the number of triangles in a linear algebraic way.



B^3

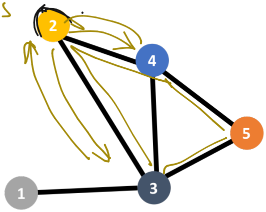
0	1	4	2	1
1	2	6	5	2
4	6	4	6	6
2	5	6	4	5
1	2	6	5	2

- B_{ij} indicates the number of 1-step paths (edges) from i, j
- $[B^2]_{ij}$ indicates the number of 2-step paths from i, j
- $[B^3]_{ij}$ indicates the number of 3-step paths from i, j

Motivating Example

Can use the adjacency matrix $B \in \{0,1\}^{n \times n}$ to write the number of triangles in a linear algebraic way.

length 4-paths from i to i
$= 2 \cdot \#$ squares i is in
$+ d_i^2$



B^3

0	1	4	2	1
1	2	6	5	2
4	6	4	6	6
2	5	6	4	5
1	2	6	5	2

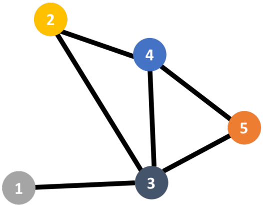
$$\frac{0+2+4+4+2}{6} = \boxed{2}$$

- B_{ij} indicates the number of 1-step paths (edges) from i, j
- $[B^2]_{ij}$ indicates the number of 2-step paths from i, j
- $[B^3]_{ij}$ indicates the number of 3-step paths from i, j

B_{ii} is the number of length 3-paths from i back to i. Thus,

$$\frac{1}{6}\operatorname{tr}(B^3) = \#\ \text{triangles}.$$

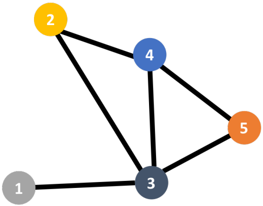
Motivating Example



$$B^3 = \begin{bmatrix} 0 & 1 & 4 & 2 & 1 \\ 1 & 2 & 6 & 5 & 2 \\ 4 & 6 & 4 & 6 & 6 \\ 2 & 5 & 6 & 4 & 5 \\ 1 & 2 & 6 & 5 & 2 \end{bmatrix}$$

$$\frac{1}{6}\,\mathrm{tr}(B^3) = \#\ \text{triangles}.$$

Motivating Example



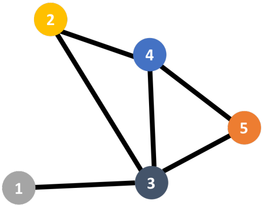
$$B^3$$

$$\begin{bmatrix} 0 & 1 & 4 & 2 & 1 \\ 1 & 2 & 6 & 5 & 2 \\ 4 & 6 & 4 & 6 & 6 \\ 2 & 5 & 6 & 4 & 5 \\ 1 & 2 & 6 & 5 & 2 \end{bmatrix}$$

$$\frac{1}{6}\,\mathrm{tr}(B^3) = \#\ \text{triangles.}$$

- Explicitly forming B^3 and computing $\mathrm{tr}(B^3)$ takes $O(n^3)$ time.

Motivating Example



B^3

0	1	4	2	1
1	2	6	5	2
4	6	4	6	6
2	5	6	4	5
1	2	6	5	2

$$\frac{1}{6}\operatorname{tr}(B^3) = \#\text{ triangles.}$$

$B^3 x = B(B(Bx))$

- Explicitly forming B^3 and computing $\operatorname{tr}(B^3)$ takes $O(n^3)$ time.
- Can multiply B^3 by a vector in $3 \cdot |E| = O(n^2)$ operations.
- So a trace estimation algorithm using m queries, yields an $O(m \cdot |E|)$ time approximate triangle counting algorithm.

$= O(m \cdot n^2)$

Example 2: Hessian/Jacobian matrix-vector products.

- For vector x, $\nabla \mathbf{f}(y)x$ and $\nabla^2 f(y)x$ can often be computed efficiently using finite difference methods or explicit differentiation (e.g., via backpropagation).
- Do not need to fully form $\nabla f(y)$ or $\nabla^2 f(y)$.
- Many applications, e.g., in analyzing neural network convergence.

Other Examples

Example 3: A is a function of another (explicit) matrix B, $A = f(B)$ that can be applied efficiently via an iterative method.

Other Examples

Example 3: A is a function of another (explicit) matrix B, $A = f(B)$ that can be applied efficiently via an iterative method.

$f(x) = x^3$

$A = f(B)$

- Repeated multiplication to apply $A = B^3$.
- Conjugate gradient, MINRES, or any linear system solver:

$$A = B^{-1}.$$

- Lanczos method, polynomial/rational approximation:

$$A = \exp(B),\ A = \sqrt{B},\ A = \log(B),\ \text{etc.}$$

- These methods run in $n^2 \cdot C$ time, where C depends on properties of B. Typically $C \ll n$ so $n^2 \cdot C \ll n^3$.

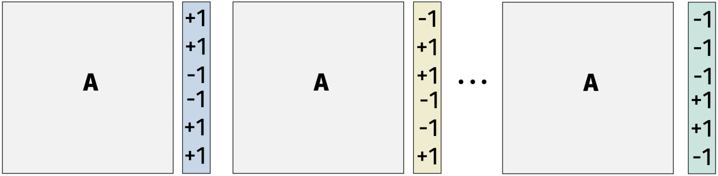
Matrix Function Examples

- Log-likelihood computation in Bayesian optimization, experimental design. $\text{tr}(\log(B)) = \log\det(B)$.
- Estrada index, a measure of protein folding degree and more generally, network connectivity. $\text{tr}(\exp(B))$.
- Trace inverse, which is important in uncertainty quantification and many other scientific computing applications. $\text{tr}(B^{-1})$
- Information about the matrix eigenvalue spectrum, since $\text{tr}(f(B)) = \sum_{i=1}^{n} f(\lambda_i)$, where λ_i is B's i^{th} eigenvalue.
- E.g., counting the number of eigenvalues in an interval, spectral density estimation, matrix norms
- See e.g., [Ubaru, and Saad 2017].

Hutchinson's Method

Hutchinson 1991, Girard 1987:

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathrm{T}} = \frac{1}{m} \sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.



- One of the earliest examples of a randomized algorithm for linear algebraic computation.

Hutchinson's Method Error Bound

Theorem

Let $\overline{\mathsf{T}}$ be the trace estimate returned by Hutchinson's method. If $m = O\left(\frac{1}{\delta\epsilon^2}\right)$, then with probability $\geq 1 - \delta$,

$$\left|\overline{\mathsf{T}} - \mathrm{tr}(A)\right| \leq \epsilon \|A\|_F$$

Hutchinson's Method Error Bound

Theorem

Let $\bar{\mathsf{T}}$ be the trace estimate returned by Hutchinson's method. If $m = O\left(\frac{1}{\delta\epsilon^2}\right)$, then with probability $\geq 1-\delta$,

$$\left|\bar{\mathsf{T}} - \mathrm{tr}(A)\right| \leq \epsilon\|A\|_F$$

$$\leq \varepsilon \, tr(A)$$

If A is symmetric positive semidefinite (PSD) then

$$\|A\|_F = \sqrt{\sum_{i=1}^{n} \lambda_i^2} \leq \sum_{i=1}^{n} \lambda_i = \mathrm{tr}(A).$$

So for PSD A: $(1-\epsilon)\,\mathrm{tr}(A) \leq \bar{\mathsf{T}} \leq (1+\epsilon)\,\mathrm{tr}(A).$

Proof Approach

Theorem

Let $\overline{\mathsf{T}}$ be the trace estimate returned by Hutchinson's method. If $m = O\left(\frac{1}{\delta\epsilon^2}\right)$, then with probability $\geq 1 - \delta$,

$$\left|\overline{\mathsf{T}} - \mathrm{tr}(A)\right| \leq \epsilon \|A\|_F$$

1. Show that $\mathbb{E}[\overline{\mathsf{T}}] = \mathrm{tr}(A)$.
2. Bound $\mathrm{Var}[\overline{\mathsf{T}}]$.
3. Apply Chebyshev's inequality.

Proof Approach

Theorem

Let $\bar{\mathsf{T}}$ be the trace estimate returned by Hutchinson's method. If $m = O\left(\frac{1}{\delta\epsilon^2}\right)$, then with probability $\geq 1-\delta$,

$$\left|\bar{\mathsf{T}} - \text{tr}(A)\right| \leq \epsilon\|A\|_F$$

$\frac{1}{t}\sum x_i^T A x_i$

1. Show that $\mathbb{E}[\bar{\mathsf{T}}] = \text{tr}(A)$.
2. Bound $\text{Var}[\bar{\mathsf{T}}]$.
3. Apply Chebyshev's inequality.

A tighter proof that uses the Hanson-Wright inequality, an exponential concentration inequality for quadratic forms, can improve the δ dependence to $\log(1/\delta)$.

Expectation Analysis

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathsf{T}} = \frac{1}{m} \sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

By linearity of expectation, $\mathbb{E}[\bar{\mathsf{T}}] = \mathbb{E}[\mathbf{x}^T A \mathbf{x}]$ for a single random ± 1 vector $\mathbf{x}$.

Expectation Analysis

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathsf{T}} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\operatorname{tr}(A)$.

By linearity of expectation, $\mathbb{E}[\bar{\mathsf{T}}] = \mathbb{E}[\mathbf{x}^T A \mathbf{x}]$ for a single random ± 1 vector $\mathbf{x}$.

non a random variable

$$\mathbb{E}[\mathbf{x}^T A \mathbf{x}] = \mathbb{E}\sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{x}_i \mathbf{x}_j A_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij} \cdot \mathbb{E}[\mathbf{x}_i \mathbf{x}_j]$$

$i \neq j \quad \mathbb{E}[x_i] \cdot \mathbb{E}[x_j] = 0$

$i = j \quad \mathbb{E} x_i x_j = \mathbb{E} x_i^2 = 1$

Expectation Analysis

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathsf{T}} = \frac{1}{m}\sum_{i=1}^m \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\text{tr}(A)$.

By linearity of expectation, $\mathbb{E}[\bar{\mathsf{T}}] = \mathbb{E}[\mathbf{x}^T A \mathbf{x}]$ for a single random ± 1 vector $\mathbf{x}$.

$$\mathbb{E}[\mathbf{x}^T A \mathbf{x}] = \mathbb{E}\sum_{i=1}^n \sum_{j=1}^n \mathbf{x}_i \mathbf{x}_j A_{ij} = \sum_{i=1}^n \sum_{j=1}^n A_{ij} \cdot \mathbb{E}[\mathbf{x}_i \mathbf{x}_j]$$

- When $i \neq j$, $\mathbf{x}_i \mathbf{x}_j = 1$ with probability 1/2 and -1 with probability 1/2, so $\mathbb{E}[\mathbf{x}_i \mathbf{x}_j] = 0$. When $i = j$, $\mathbf{x}_i \mathbf{x}_j = 1$, so $\mathbb{E}[\mathbf{x}_i \mathbf{x}_j] = 1$.

Expectation Analysis

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathrm{T}} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

By linearity of expectation, $\mathbb{E}[\bar{\mathrm{T}}] = \mathbb{E}[\mathbf{x}^T A \mathbf{x}]$ for a single random ± 1 vector $\mathbf{x}$.

$$\mathbb{E}[\mathbf{x}^T A \mathbf{x}] = \mathbb{E}\sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{x}_i \mathbf{x}_j A_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij} \cdot \mathbb{E}[\mathbf{x}_i \mathbf{x}_j] = \sum_{i=1}^{n} A_{ii}. \quad = \mathrm{tr}(A).$$

- When $i \neq j$, $\mathbf{x}_i \mathbf{x}_j = 1$ with probability $1/2$ and -1 with probability $1/2$, so $\mathbb{E}[\mathbf{x}_i \mathbf{x}_j] = 0$. When $i = j$, $\mathbf{x}_i \mathbf{x}_j = 1$, so $\mathbb{E}[\mathbf{x}_i \mathbf{x}_j] = 1$.

Expectation Analysis

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathsf{T}} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\text{tr}(A)$.

By linearity of expectation, $\mathbb{E}[\bar{\mathsf{T}}] = \mathbb{E}[\mathbf{x}^T A \mathbf{x}]$ for a single random ± 1 vector $\mathbf{x}$.

$$\mathbb{E}[\mathbf{x}^T A \mathbf{x}] = \mathbb{E} \sum_{i=1}^{n} \sum_{j=1}^{n} \mathbf{x}_i \mathbf{x}_j A_{ij} = \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} \cdot \mathbb{E}[\mathbf{x}_i \mathbf{x}_j] = \sum_{i=1}^{n} A_{ii}.$$

- When $i \neq j$, $\mathbf{x}_i \mathbf{x}_j = 1$ with probability $1/2$ and -1 with probability $1/2$, so $\mathbb{E}[\mathbf{x}_i \mathbf{x}_j] = 0$. When $i = j$, $\mathbf{x}_i \mathbf{x}_j = 1$, so $\mathbb{E}[\mathbf{x}_i \mathbf{x}_j] = 1$.
- So the estimator is correct in expectation: $\mathbb{E}[\bar{\mathsf{T}}] = \text{tr}(A)$.

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathsf{T}} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

$$\mathrm{Var}[\bar{\mathsf{T}}]$$

Variance Bound

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathrm{T}} = \frac{1}{m} \sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

$$\mathrm{Var}[\bar{\mathrm{T}}] = \frac{1}{m} \mathrm{Var}[\mathbf{x}^T A \mathbf{x}]$$

Variance Bound

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathsf{T}} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

$$\mathrm{Var}[\bar{\mathsf{T}}] = \frac{1}{m}\mathrm{Var}[\mathbf{x}^T A \mathbf{x}] = \frac{1}{m}\mathrm{Var}\left[\sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{x}_i \mathbf{x}_j A_{ij}\right]$$

Variance Bound

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathrm{T}} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

$$\mathrm{Var}[\bar{\mathrm{T}}] = \frac{1}{m}\mathrm{Var}[\mathbf{x}^T A \mathbf{x}] = \frac{1}{m}\mathrm{Var}\left[\underbrace{\sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{x}_i \mathbf{x}_j A_{ij}}_{\text{terms are not quite independent.}}\right]$$

Can we apply linearity of variance here?

$x_i x_j A_{ij} \qquad x_i x_j A_{ji}$

$x_i x_j (A_{ij} + A_{ji})$

$\{x_i x_j\}_{i,j}$ are pair wise independent but not fully independent.

$x_1 x_2 \quad x_1 x_3 \quad x_2 x_3$

$x_1^2 \cdot x_2 \cdot x_3 = x_2 \cdot x_3$

Variance Bound

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\overline{\mathrm{T}} = \frac{1}{m} \sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

$$\mathrm{Var}[\overline{\mathrm{T}}] = \frac{1}{m} \mathrm{Var}[\mathbf{x}^T A \mathbf{x}] = \frac{1}{m} \mathrm{Var}\left[\sum_{i=1}^{n} \sum_{j=1}^{n} \mathbf{x}_i \mathbf{x}_j A_{ij}\right]$$

Can we apply linearity of variance here? Almost – need to remove repeated terms, and then can use pairwise independence.

Variance Bound

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathrm{T}} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

$$\mathrm{Var}[\bar{\mathrm{T}}] = \frac{1}{m}\mathrm{Var}[\mathbf{x}^T A \mathbf{x}] = \frac{1}{m}\mathrm{Var}\left[\sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{x}_i \mathbf{x}_j A_{ij}\right]$$

Can we apply linearity of variance here? Almost – need to remove repeated terms, and then can use pairwise independence.

fixed

$$\mathrm{Var}[\bar{\mathrm{T}}] = \frac{1}{m}\mathrm{Var}\left[\cancel{\sum_{i=1}^{n} A_{ii}} + \sum_{i=1}^{n}\sum_{j>i} \mathbf{x}_i \mathbf{x}_j (A_{ij} + A_{ji})\right]$$

Variance Bound

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathsf{T}} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\operatorname{tr}(A)$.

$$\operatorname{Var}[\bar{\mathsf{T}}] = \frac{1}{m}\operatorname{Var}[\mathbf{x}^T A \mathbf{x}] = \frac{1}{m}\operatorname{Var}\left[\sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{x}_i \mathbf{x}_j A_{ij}\right]$$

Can we apply linearity of variance here? Almost – need to remove repeated terms, and then can use pairwise independence.

$$\operatorname{Var}[\bar{\mathsf{T}}] = \frac{1}{m}\operatorname{Var}\left[\sum_{i=1}^{n} A_{ii} + \sum_{i=1}^{n}\sum_{j>i} \mathbf{x}_i \mathbf{x}_j \underbrace{(A_{ij} + A_{ji})}\right]$$

$$= \frac{1}{m}\sum_{i=1}^{n}\sum_{j>i} \operatorname{Var}[\underbrace{\mathbf{x}_i \mathbf{x}_j}_{\pm 1}] \cdot (A_{ij} + A_{ji})^2$$

Variance Bound

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathsf{T}} = \frac{1}{m} \sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\operatorname{tr}(A)$.

$$\mathrm{Var}[\bar{\mathsf{T}}] = \frac{1}{m} \mathrm{Var}[\mathbf{x}^T A \mathbf{x}] = \frac{1}{m} \mathrm{Var}\left[\sum_{i=1}^{n} \sum_{j=1}^{n} \mathbf{x}_i \mathbf{x}_j A_{ij}\right]$$

Can we apply linearity of variance here? Almost – need to remove repeated terms, and then can use pairwise independence.

$$\mathrm{Var}[\bar{\mathsf{T}}] = \frac{1}{m} \mathrm{Var}\left[\sum_{i=1}^{n} A_{ii} + \sum_{i=1}^{n} \sum_{j>i} \mathbf{x}_i \mathbf{x}_j (A_{ij} + A_{ji})\right]$$

$$= \frac{1}{m} \sum_{i=1}^{n} \sum_{j>i} \mathrm{Var}[\mathbf{x}_i \mathbf{x}_j] \cdot (A_{ij} + A_{ji})^2 \leq \frac{1}{m} \sum_{i=1}^{n} \sum_{j>i} 2A_{ij}^2 + 2A_{ji}^2$$

Variance Bound

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\bar{\mathrm{T}} = \frac{1}{m}\sum_{i=1}^m \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

$$\mathrm{Var}[\bar{\mathrm{T}}] = \frac{1}{m}\mathrm{Var}[\mathbf{x}^T A \mathbf{x}] = \frac{1}{m}\mathrm{Var}\left[\sum_{i=1}^n \sum_{j=1}^n \mathbf{x}_i \mathbf{x}_j A_{ij}\right]$$

Can we apply linearity of variance here? Almost – need to remove repeated terms, and then can use pairwise independence.

$$\mathrm{Var}[\bar{\mathrm{T}}] = \frac{1}{m}\mathrm{Var}\left[\sum_{i=1}^n A_{ii} + \sum_{i=1}^n \sum_{j>i} \mathbf{x}_i \mathbf{x}_j (A_{ij} + A_{ji})\right]$$

$$= \frac{1}{m}\sum_{i=1}^n \sum_{j>i} \mathrm{Var}[\mathbf{x}_i \mathbf{x}_j] \cdot (A_{ij} + A_{ji})^2 \leq \frac{1}{m}\sum_{i=1}^n \sum_{j>i} 2A_{ij}^2 + 2A_{ji}^2 \leq \frac{2\|A\|_F^2}{m}.$$

Final Analysis

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\overline{\mathsf{T}} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

Chebyshev's inequality implies that, for $m = \frac{2}{\delta\epsilon^2}$:

$$\Pr\left[\left|\overline{\mathsf{T}} - \mathrm{tr}(A)\right| \geq \epsilon\|A\|_F\right] \leq \frac{2\|A\|_F^2/m}{\epsilon^2\|A\|_F^2} = \delta.$$

Final Analysis

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\overline{\mathsf{T}} = \frac{1}{m} \sum_{i=1}^m \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

Chebyshev's inequality implies that, for $m = \frac{2}{\delta \epsilon^2}$:

$$\Pr\left[\left|\overline{\mathsf{T}} - \mathrm{tr}(A)\right| \geq \epsilon \|A\|_F\right] \leq \frac{2\|A\|_F^2/m}{\epsilon^2 \|A\|_F^2} = \delta.$$

Could we have gotten a better bound by applying Bernstein's inequality to $\sum_{i=1}^n \sum_{j>i} \mathbf{x}_i \mathbf{x}_j (A_{ij} + A_{ji})$? – No because we only have pairwise independence

Final Analysis

Hutchinson's Estimator::

- Draw $\mathbf{x}_1, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ i.i.d. with random $\{+1, -1\}$ entries.
- Return $\overline{\mathsf{T}} = \frac{1}{m}\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i$ as an approximation to $\mathrm{tr}(A)$.

Chebyshev's inequality implies that, for $m = \frac{2}{\delta\epsilon^2}$:

$$\Pr\left[\left|\overline{\mathsf{T}} - \mathrm{tr}(A)\right| \geq \epsilon\|A\|_F\right] \leq \frac{2\|A\|_F^2/m}{\epsilon^2\|A\|_F^2} = \delta.$$

Could we have gotten a better bound by applying Bernstein's inequality to $\sum_{i=1}^{n}\sum_{j>i}\mathbf{x}_i\mathbf{x}_j(A_{ij} + A_{ji})$?

Hanson-Wright is an exponential concentration bound that can be used in the specific case – improves bound to $m = O\left(\frac{\log(1/\delta)}{\epsilon^2}\right)$.

Optimality of Hutchinson's Method

The $m = O\left(\frac{\log(1/\delta)}{\epsilon^2}\right)$ bound given by the Hanson-Wright inequality is tight.

- Any algorithm that only uses queries of the form $\mathbf{x}_i^T A \mathbf{x}_i$ requires $\Omega\left(\frac{\log(1/\delta)}{\epsilon^2}\right)$ samples to estimate $\mathrm{tr}(A)$ to error $\pm\epsilon\,\mathrm{tr}(A)$ for PSD A [Wimmer, Wu, Zhang 2014].

Optimality of Hutchinson's Method

The $m = O\left(\frac{\log(1/\delta)}{\epsilon^2}\right)$ bound given by the Hanson-Wright inequality is tight.

- Any algorithm that only uses queries of the form $\mathbf{x}_i^T A \mathbf{x}_i$ requires $\Omega\left(\frac{\log(1/\delta)}{\epsilon^2}\right)$ samples to estimate $\text{tr}(A)$ to error $\pm\epsilon\,\text{tr}(A)$ for PSD A [Wimmer, Wu, Zhang 2014].
- We recently showed that using the full power of matrix-vector queries, one can achieve $O\left(\frac{\log(1/\delta)}{\epsilon}\right)$ queries for PSD matrices – see project topics.