In the next few classes, we will discuss randomized numerical linear algebra (RandNLA) and its applications to a number of problems. In this lecture we consider the problem of approximate matrix multiplication, and then begin a discussion on the problem of least squared approximation.

1 Introduction

In RandNLA, we develop randomized algorithms for several fundamental numerical linear algebra tasks:

1. Approximate matrix multiplication (Today)
2. Least squares approximation (Today and next lecture)
3. Low-rank matrix approximation
4. (Not this semester) Graph sparsification

We will focus on the first three problems. Note that techniques developed in Problem 1 will be used in Problem 2, which in turn will be used in Problem 3.

1.1 Efficient large-scale data processing

When processing large-scale data (in particular, streaming data), we desire methods that can be performed with

- a few (e.g., one or two) passes of data
- limited memory (complete data might not fit in memory)
- low time complexity

A general idea is RandNLA is to use randomization to get a rough sketch of the data. There are two main approaches:

- **Random (down)sampling**: randomly select a subset of data
  - Pros: Easy to implement
  - Cons: Quality often depends on property of data

- **Random projection**: rotates / projects data to lower dimensions
  - Pros: Often data-agnostic, more robust
  - Cons: More computationally expensive

See Figure 1 for an illustrations of the pros and cons of these two approaches.

On a high level, RandNLA involves randomized algorithm + matrix concentration/perturbation theory. Note that Probability used in algorithm and analysis (previously only used in analysis). Applications of RandNLA include

---

1 Reading: [Mahoney, 2016]: “Lecture notes on randomized linear algebra. Available at https://arxiv.org/abs/1608.04481
2 We thank Yuxin Chen for allowing us to draw from his slides for ELE 520: Mathematics of Data Science, Princeton University, Fall 2020.
Consider estimating $\sum \|x_i\|$ for the points below by random sampling. In order for the estimate to be accurate we need to include the red outlier point, for instance by increasing sampling weight for red point. On the other hand, random projections preserve more information from data.

- Scientific computing;
- Machine learning: e.g., PCA on ≥terabyte-sized problems.

2 Faster Matrix Multiplication

Given $A \in \mathbb{R}^{m \times n}$ and $B \in \mathbb{R}^{n \times p}$, compute or approximate $AB$. A native algorithm for exactly computing $AB$ is given in Algorithm 1.

Algorithm 1: Vanilla algorithm for matrix multiplication

1: for $i = 1, \ldots, m$ do
2: for $k = 1, \ldots, n$ do
3: $M_{i,k} = A_{i,:}B_{:,k}$
4: return $M$

The computational complexity of Algorithm 1 is $O(mnp)$, or $O(n^3)$ if $m = n = p$. For simplicity, we shall assume $m = n = p$ in the sequel unless otherwise noted.

There exists algorithms with sub-cubic time complexity, such as the Strassen algorithm for exact matrix multiplication. The asymptotic computational complexity is $\approx O(n^{2.8})$. For various reasons, this algorithm is not commonly used in practice.

Our general goal is to develop randomized algorithm with time complexity $= \tilde{O}(n^2).$

2.1 A Simple Randomized Algorithm

We view $AB$ as a sum of rank-one matrices (or outer products)

$$AB = \sum_{i=1}^{n} A_{i,:}B_{:,i}.\$$

Our idea is to randomly sample $L$ rank-one components. This leads to Algorithm 2
Algorithm 2: Basic randomized algorithm for matrix multiplication

```
1: for \( l = 1, \ldots, L \) do
2: \quad Pick \( i_l \in \{1, \ldots, n\} \) i.i.d. with probability \( \mathbb{P}\{i_l = k\} = p_k \)
3: \quad return
M = \frac{1}{L} \sum_{l=1}^{L} \frac{1}{p_{i_l}} A_{:i_l} B_{i_l:}
```

A few remarks for Algorithm 2

- \( \{p_k : k = 1, \ldots, n\} \) are called *importance sampling probabilities*.
- \( M \) is an *unbiased* estimate of \( AB \), i.e.,
  \[
  \mathbb{E}[M] = AB.
  \]
- The approximation error (e.g., \( \|M - AB\| \)) depends on \( \{p_k\} \).

### 2.2 Importance Sampling Probabilities

There are two ways for choosing the probabilities \( \{p_k : k = 1, \ldots, n\} \). The simplest one is:

- **Uniform sampling**
  \[ p_k = \frac{1}{n}. \]
  Here one can sample the index set \( \{i_1, \ldots, i_L\} \) before looking at data, so it’s implementable via one pass over data.
  Intuitively, one may prefer biasing towards larger rank-1 components. This suggests that we can use

- **Non-uniform sampling**
  \[ p_k = \frac{\|A_{:k}\|_2 \|B_{k:}\|_2}{\sum_{l=1}^{n} \|A_{:l}\|_2 \|B_{l:}\|_2} \]
  Note that the probabilities \( \{p_k\} \) can be computed using one pass and \( O(n) \) memory. Nonuniform sampling favors “larger” rank 1 matrices, with sampling probabilities proportional to
  \[ \|A_{:k} B_{k:}\|_{op} = \|A_{:k}\|_2 \|B_{k:}\|_2. \]
  It turns out the nonuniform sampling probabilities above are optimal with respect to the mean squared approximation error \( \mathbb{E}[\|M - AB\|_F^2] \).

**Lemma 1.** \( \mathbb{E}[\|M - AB\|_F^2] \) is minimized by

\[
p_k = \frac{\|A_{:k}\|_2 \|B_{k:}\|_2}{\sum_{l=1}^{n} \|A_{:l}\|_2 \|B_{l:}\|_2}.
\]

- Consequently, we call (1) the optimal sampling probabilities (w.r.t. mean squared error)
Proof Since \( E[M] = AB \), one has

\[
E \left[ \| M - AB \|_F^2 \right] = E \left[ \sum_{i,j} (M_{i,j} - A_{i,:} B_{:j})^2 \right] = \sum_{i,j} \text{Var}[M_{i,j}]
\]

\[
= \frac{1}{L} \sum_k \sum_{i,j} \frac{A_{i,k} B_{k,j}^2}{p_k} - \frac{1}{L} \sum_{i,j} (A_{i,:} B_{:j})^2 \quad \text{(check)}
\]

\[
= \frac{1}{L} \sum_k \frac{1}{p_k} \| A_{i,k} \|_2^2 \| B_{k,:} \|_2^2 - \frac{1}{L} \| AB \|_F^2
\]

(2)

In addition, Cauchy-Schwarz yields \((\sum_k p_k) \left( \sum_k \alpha_k p_k \right) \geq (\sum_k \sqrt{\alpha_k})^2\), with equality attained if \( p_k \propto \sqrt{\alpha_k} \). Setting \( \alpha_k = \| A_{i,k} \|_2^2 \| B_{k,:) \|_2^2 \) gives

\[
E \left[ \| M - AB \|_F^2 \right] \geq \frac{1}{L} \left( \sum_k \| A_{i,k} \|_2 \| B_{k,:) \|_2 \right)^2 - \frac{1}{L} \| AB \|_F^2,
\]

where the lower bound is achieved when \( p_k \propto \| A_{i,k} \|_2 \| B_{k,:) \|_2 \)

\[ \Box \]

2.3 Error Concentration

The previous analysis concerns \( E[\| M - AB \|_F^2] \), i.e., the approximation error in expectation. In practice, one often hopes, in addition, that \( M \) is close to \( AB \) most of the time. Thus, we desire an error bound that holds with high probability.

- Frobenius norm error: \( \| M - AB \|_F \), and
- spectral norm error: \( \| M - AB \| \).

Our general idea is to invoke matrix concentration inequalities to control these metrics. To this end, recall the Matrix Bernstein inequality.

**Theorem 1** (Matrix Bernstein). Let \( \{X_i \in \mathbb{R}^{d_1 \times d_2}, i = 1, \ldots, L \} \) be a sequence of independent zero-mean random matrices. Assume

\[
\begin{align*}
\text{(range)} & \quad \|X_i\| \leq R, \quad \forall i = 1, \ldots, L, \\
\text{(variance)} & \quad \text{max} \left\{ \| \mathbb{E} \left[ \sum_{l=1}^L X_i X_i^\top \right] \|, \| \mathbb{E} \left[ \sum_{l=1}^L X_i^\top X_i \right] \| \right\} \leq V.
\end{align*}
\]

Then,

\[
P \left\{ \| \sum_{l=1}^L X_i \| \geq \tau \right\} \leq (d_1 + d_2) \exp \left( \frac{-\tau^2/2}{V + R \tau^3/3} \right)
\]

2.4 Frobenius Norm Error

We have the following bound on the approximation error in Frobenius norm.

**Theorem 2** (Frobenius Norm Error of Matrix Multiplication). Suppose \( p_k \geq \frac{\beta \| A_{i,k} \|_2 \| B_{k,:) \|_2}{\sum \| A_{i,k} \|_2 \| B_{k,:) \|_2} \), \( \forall k \) for some \( \beta \in (0,1) \). If \( L \geq \frac{\log n}{\beta} \), then the estimate \( M \) returned by Algorithm 2 obeys

\[
\| M - AB \|_F \lesssim \sqrt{\frac{\log n}{\beta L} \| A \|_F \| B \|_F}
\]

with probability at least \( 1 - O(n^{-10}) \).
Proof. Observe that $\text{vec}(M) = \sum_{l=1}^{L} X_l$, where $X_l = \sum_{k=1}^{n} \frac{1}{Lp_k} A_{:,k} \otimes B_{k,:}^\top \mathbb{1}_{i_l = k}$. These matrices $\{X_l\}$ obey
\[
\|X_l\|_2 \leq \max_k \frac{1}{Lp_k} \|A_{:,k}\|_2 \|B_{k,:}\|_2 \approx \frac{1}{\beta L} \sum_{k=1}^{n} \|A_{:,k}\|_2 \|B_{k,:}\|_2 =: R.
\]
(3)
\[
\mathbb{E} \left[ \sum_{l=1}^{L} \|X_l\|_2^2 \right] = L \sum_{k=1}^{n} \mathbb{P} \{i_l = k\} \frac{\|A_{:,k}\|_2^2 \|B_{k,:}\|_2^2}{L^2 p_k^2} \leq \frac{1}{\beta L} \left( \sum_{k=1}^{n} \|A_{:,k}\|_2 \|B_{k,:}\|_2 \right)^2.
\]
(4)

We then invoke matrix Bernstein to obtain
\[
\|M - AB\|_F = \left\| \sum_{l=1}^{L} (X_l - \mathbb{E}[X_l]) \right\|_2 \lesssim \sqrt{V \log n + R \log n}.
\]
\[
\lesssim \sqrt{\log n + R \log n} \leq \sqrt{\frac{\log n}{\beta L} \left( \sum_{k=1}^{n} \|A_{:,k}\|_2 \|B_{k,:}\|_2 \right)}.
\]
\[
\leq \sqrt{\frac{\log n}{\beta L} \|A\|_F \|B\|_F} \quad \text{(Cauchy-Schwarz)}
\]

A few remarks on Theorem 2:

• If $L \gtrsim \frac{\log n}{\varepsilon^2 \beta}$, then $\|M - AB\|_F \lesssim \varepsilon \|A\|_F \|B\|_F$.

• Time complexity: $O\left(\frac{n^2}{\varepsilon^2} + \frac{\log n}{\varepsilon^2} \right)$. Note that this is one of the few cases where the time complexity can be readily estimated. For more complex problems, bounding time complexity requires more careful arguments and in particular is implementation dependent.

• The proof above highlights why nonuniform sampling probabilities is useful. If we instead use the probabilities $p_k = \frac{1}{n}$, then equation (3) would become $\max_k \frac{n}{2} \|A_{:,k}\|_2 \|B_{k,:}\|_2$, from which Matrix Bernstein will result in a worst error bound.

2.5 Spectral Norm Error

We also have the following bound on the approximation error in spectral norm. For simplicity, we consider the simpler problem of approximating $AA^\top$ (i.e., $B = A^\top$).

Theorem 3. Suppose $p_k \geq \frac{\beta \|A_{:,k}\|_2}{\|A\|_F^2}$, $\forall k$ for some quantity $0 < \beta \leq 1$, and $L \gtrsim \frac{\|A\|_F^2}{\beta \|A\|_F^2 \log n}$. Then the estimate $M$ returned by Algorithm 2 obeys
\[
\|M - AA^\top\| \lesssim \sqrt{\frac{\log n}{\beta L} \|A\|_F \|A\|}.
\]
with prob. at least $1 - O(n^{-10})$. 

5
Proof. Write \( M = \sum_{l=1}^{L} Z_l \), where \( Z_l = \sum_{k=1}^{n} \frac{1}{Lp_k} A_{:,k} A_{:,k}^\top 1 \{i_l = k\} \). These matrices satisfy

\[
\|Z_l\|_2 \leq \max_k \frac{\|A_{:,k}\|_2^2}{Lp_k} \leq \frac{1}{\beta L} \|A\|_F^2 : = R
\]

\[
\left\| \mathbb{E} \left[ \sum_{l=1}^{L} Z_l Z_l^\top \right] \right\| = \left\| L \sum_{k=1}^{n} \mathbb{P} \{i_l = k\} \frac{\|A_{:,k}\|_2^2}{L^2 p_k} A_{:,k} A_{:,k}^\top \right\|
\leq \frac{1}{\beta L} \|A\|_F^2 \|AA^\top\|
= \frac{1}{\beta L} \|A\|_F^2 \|A\|^2 = : V
\]

Invoke matrix Bernstein to conclude that with high prob.,

\[
\|M - AA^\top\| = \left\| \sum_{l=1}^{L} (Z_l - \mathbb{E}[Z_l]) \right\| \lesssim \sqrt{V \log n} + B \log n
\]

\[
\geq \frac{\log n}{\beta L} \|A\|_F \|A\|
\]

A few remarks on Theorem 3:

- The error bound depends on \( \|A\|_F \|A\| \). In comparison, the Frobenius error bound in Theorem 2 involves \( \|A\|_F^2 \).

- If \( L \gtrsim \frac{\|A\|_F^2 \log n}{\|A\|_F^2} \), then \( \|M - AA^\top\| \lesssim \epsilon \|A\|^2 \). Here \( \frac{\|A\|_F^2}{\|A\|_F^2} \) is called the stable rank of the matrix \( A \). For approximately low rank matrices the stable rank \( \approx 1 \); for high rank matrices stable rank \( \approx n \). Therefore, Theorem 3 is most useful when \( A \) is approximately low rank.

- We note that Theorem 3 is a generalization of kernel approximation bound for random features from Lecture 5.

- Can be generalized to approximate \( AB \) (Magen, Zouzias ’11) [Magen and Zouzias, 2011]

- For many problems, the spectral bound is more useful since

\[
\|M - AB\| \leq \epsilon \Rightarrow \|Mu - ABu\|_2 \leq \epsilon \|u\|_2
\]

### 2.6 Matrix Multiplication with One Sided Information

What if we only use the information about \( A \) (but not \( B \))?

- This situation arises when \( B \) is defined implicitly, e.g., as the solution to optimization problem.

- We will later see an example of this situation in approximate least squares with nonuniform sampling.

Suppose we choose the sample probabilities as \( p_k \geq \frac{\beta \|A\|_F^2}{\|A\|_F^2} \). In this case, matrix Bernstein does NOT give good concentration bounds. In particular, we will get a poor bound in equation (3):

\[
R \propto \max_k \frac{\|B_{:,k}\|_2}{\|A_{:,k}\|_2} \|A\|_F^2.
\]

Can be large
Nevertheless, we can still use Markov’s inequality to get some useful bound. More precisely, when \( p_k \geq \frac{\beta \| A_{:,k} \|_F^2}{\| B_{:,k} \|_2^2} \), it follows from (2) that

\[
\mathbb{E} \left[ \| M - AB \|_F^2 \right] = \frac{1}{L} \sum_k \frac{1}{p_k} \| A_{:,k} \|_2^2 \| B_{:,k} \|_2^2 - \frac{1}{L} \| AB \|_F^2 \leq \frac{1}{\beta L} \left( \sum_k \| B_{:,k} \|_2^2 \right) \| A \|_F^2 = \frac{\| A \|_F^2 \| B \|_F^2}{\beta L}.
\]

Hence, Markov’s inequality yields that with prob. at least \( 1 - \frac{1}{\log n} \),

\[
\| M - AB \|_F^2 \leq \frac{\| A \|_F^2 \| B \|_F^2 \log n}{\beta L},
\]

(5)

Note that the probability is worse compared to Theorem 2, which gives \( 1 - \frac{1}{n^{10}} \).

3 Least Squares Approximation

We next turn to the least squares (LS) problem.

3.1 Least Squares Problem

Given \( A \in \mathbb{R}^{n \times d} \) \((n \gg d)\) and \( b \in \mathbb{R}^n \), the goal is to find the solution \( x_{ls} \) to the optimization problem

\[
\text{minimize}_{x \in \mathbb{R}^d} \quad \| Ax - b \|_2.
\]

See Figure 2 for a geometric interpretation of the least squares problem, which is equivalent to computing the orthogonal projection of \( b \) onto range(\( A \)) (the column space of \( A \)). The least squares solution \( x_{ls} \) satisfies \((Ax_{ls} - b) \perp \text{range}(A)\).

![Diagram of least squares](image)

Figure 2: Geometric picture of least squares

Algebraically, \( x_{ls} \) satisfies the normal equation

\[
A^T Ax_{ls} = A^T b, \quad \text{or equivalently} \quad A^T (Ax_{ls} - b) = 0.
\]
If $A$ has full column rank, then $x_{ls}$ is given in closed form:

$$x_{ls} = (A^\top A)^{-1} A^\top b = V_A \Sigma_A^{-1} U_A^\top b,$$

where $A = U_A \Sigma_A V_A^\top$ is the SVD of $A$, and $A^\dagger$ is called the pseudo inverse of $A$ (as $A^\dagger A = I_d$).

### 3.2 Methods for Solving LS Problems

In practice, one rarely uses the close-form expression $(A^\top A)^{-1} A^\top b$ to compute the least squares solution $x_{ls}$, as it involves forming and inverting the matrix $A^\top A$, which is costly and unnecessary.

Instead, one typically uses one of the following two main classes of method for computing $x_{ls}$.

**Direct methods:** these are variants of Gaussian elimination. The computational complexity is roughly $O(nd^2)$. Examples of direct methods include:

- **Cholesky decomposition:** compute upper triangular matrix $R$ s.t. $A^\top A = R^\top R$, and solve $R^\top Rx = A^\top b$
- **QR decomposition:** compute QR decomposition $A = QR$ ($Q$: orthonormal; $R$: upper triangular), and solve $Rx = Q^\top b$

Direct methods yield high accuracy solutions. These methods are often used on dense $A$.

**Iterative methods:** Example include Conjugate gradient and variants. The computational complexity is roughly $O(nd \cdot \sigma_{\max}(A) / \sigma_{\min}(A) \log \frac{1}{\epsilon})$, which is linear in $d$ and depends logarithmically on the target accuracy $\epsilon$. Such methods allow one to tradeoff between accuracy and computation cost. They are often used on large sparse $A$, for which matrix-vector product can be computed in time linear in the sparsity of $A$. However, due to the dependence on the condition number $\sigma_{\max}(A) / \sigma_{\min}(A)$, iterative methods may be slow on ill-conditioned problems.

We will instead look at randomized methods. The high-level goal is to achieve sample complexity of the form $O(nd/\epsilon^2)$, which is linear in $d$ and (hopefuly) independent of the condition number of $A$. That is, randomized algorithms have better dependence on $d$ compared to direct methods, and are still fast on ill-conditioned problem compared to iterative methods. The price we pay is a worst dependence on the target accuracy $\epsilon$.

### 3.3 Randomized LS Approximation

The **Basic idea** is to generate a sketching/sampling matrix $\Phi \in \mathbb{R}^{r \times n}$ (with $r \ll n$, e.g., via random sampling, random projection), and solve a smaller LS problem:

$$\bar{x}_{ls} = \arg \min_{x \in \mathbb{R}^d} \| \Phi (Ax - b) \|_2$$

For example, if $\Phi$ is a subsampling matrix of the form

$$\Phi \in \mathbb{R}^{2 \times n} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix},$$

then

$$\Phi A = \begin{bmatrix} A_{1,:} \\ A_{n,:} \end{bmatrix} \in \mathbb{R}^{2 \times d}$$

picks out two rows of $A$.  

Our goal is to find $\Phi$ such that $\widetilde{x}_{ls}$ approximates $x_{ls}$ in terms of the estimation error and fitting error, that is,

$$\widetilde{x}_{ls} \approx x_{ls}, \quad \|A\widetilde{x}_{ls} - b\|_2 \approx \|Ax_{ls} - b\|_2.$$ 

Before we proceed, we consider two extreme cases for the choice of $|\Phi|$.

- $\Phi = I_{n \times n}$. This $\Phi$ is easy to compute, but it does not change the LS problem and hence has no improvement for computational cost.

- $\Phi = U_A^T$. In this case, we have

$$\Phi A = U_A^T U_A \Sigma V_A^T = \underbrace{\Sigma V_A^T}_{\hat{A}'},$$

Therefore, the coefficient matrix $\Phi A = \hat{A}'$ for the subsampled LS problem (6) is a product of a diagonal and orthonormal matrix. The corresponding normal equation

$$\begin{bmatrix} \hat{A}'^T & \hat{A}' \\ \Sigma V_A^T A' \\ V_A \Sigma V_A^T \\ A' \Sigma V_A^T A' \end{bmatrix} \begin{bmatrix} \widetilde{x}_{ls} \\ A' b' \end{bmatrix} = A' b'$$

is easy to solve using direct methods. Moreover, the solution $\widetilde{x}_{ls} = x_{ls}$ is exact. However, using such $\Phi$ requires computing SVD of $A$, which is at least as hard as the original LS problem.

Our goal is to get the best of both worlds above, i.e., choose a $\Phi$ that is easy to compute and leads to a subsampled LS problem that is easier to solve than the original problem.

References
