Mathematical Toolkit **Autumn 2025**

Homework 3

Due: November 14, 2025

Note: *You may discuss these problems in groups. However, you must write up your own solutions and mention the names of the people in your group. Also, please do mention any books, papers or other sources you refer to. It is recommended that you typeset your solutions in LaTeX.*

1. **Perturbation of eigenvalues.** **[2+2+4+4]**

   In this problem, we will apply the Gershgorin disc theorem to derive a bound on the change in the eigenvalues of a matrix due to perturbation.

   (a) Two matrices $A, B \in \mathbb{C}^{n\times n}$ are called similar if there exists a non-singular matrix S such that $B = S^{-1}AS$. Show that if A and B are similar, then they have the same eigenvalues.

   (b) A matrix A is called diagonalizable if it is similar to a diagonal matrix. If A is similar to a diagonal matrix Λ, find the eigenvalues of A in terms of the entries of Λ.

   (c) Let $A \in \mathbb{C}^{n\times n}$ be a diagonalizable matrix such that $S^{-1}AS = \Lambda$ for a diagonal matrix Λ. Let $E \in \mathbb{C}^{n\times n}$ be an arbitrary matrix, which we think of as a "perturbation" of A. Let μ be an eigenvalue of $A + E$. Show that there exists an eigenvalue λ of A such that

   $$|\lambda - \mu| \;\leq\; \max_i \sum_{j=1}^{n} \left|(S^{-1}ES)_{ij}\right| .$$

   (d) Show that when A and E are both Hermitian (self-adjoint) the estimate can be improved. Note that in this case S is unitary ($S^*S = \mathsf{id}$). Prove that If $\lambda_1 \leq \cdots \leq \lambda_n$ are the eigenvalues of A, while $\mu_1 \leq \cdots \leq \cdots \mu_n$ are the eigenvalues of $A + E$, then one can get for all $i \in [n]$:

   $$|\lambda_i - \mu_i| \;\leq\; \|E\|_2 .$$

   (Recall that $\|E\|_2 = \max_{x\neq 0} \|Ex\|_2 \,/\, \|x\|_2$. Also think about why is this estimate better than the previous one.)

2. **False alarm.** **[2 + 4 + 2]**

   Consider a test for a rare genetic mutation, which is administered to an individual

chosen uniformly at random from a population of size (say) N. We define the following events

$$\begin{aligned} M &\equiv \{\text{A random individual has the genetic mutation}\} \\ T &\equiv \{\text{The test is positive}\} \end{aligned}$$

Note that the test may not be completely reliable i.e., it may not always detect the presence or absence of the mutation correctly.

(a) Define an appropriate outcome space Ω to capture the above random experiment (you don't need to specify the probability measure).

(b) Suppose we are given the following additional information:

$$\begin{aligned} \mathbb{P}[M] &= \varepsilon && (\varepsilon \text{ fraction of people have the mutation}) \\ \mathbb{P}[T^c \mid M] &= \delta_0 && (\text{Probability of a false negative is } \delta_0) \\ \mathbb{P}[T \mid M^c] &= \delta_1 && (\text{Probability of a false positive is } \delta_1) \end{aligned}$$

Calculate the probability that a person has the mutation given that the test is positive.

(c) Let $\varepsilon = \delta_0 = 1/1000$ and $\delta_1 = 1/100$. Thus, the test has a false positive rate of 1% and false negative rate of 0.1%. Calculate $\dfrac{\mathbb{P}[M|T]}{\mathbb{P}[M^c|T]}$. Is this is a reliable test for the genetic mutation?

3. **Random Polynomials.** **[2+2+2+4]**

For a prime number p, recall that the field $\mathbb{F}_p$ has the elements $\{0, 1, \ldots, p-1\}$, with addition and multiplication done modulo p. A degree-d polynomial in the variable x over the field $\mathbb{F}_p$ (for pime p) is defined as:

$$P(x) = c_0 + c_1 \cdot x + \ldots + c_d \cdot x^d ,$$

where the coefficients $c_0, \ldots, c_d$, and the variable x all take values in $\mathbb{F}_p$ (and all addition and multiplication is done modulo p). A value $x \in \mathbb{F}_p$ is called a root of P if $P(x) = 0$. Consider picking a random polynomial P by selecting $c_0, \ldots, c_d$ independently and uniformly at random from $\mathbb{F}_p$, and define the random variable

$$Z = \text{Number of roots of } P .$$

(a) Define an appropriate probability space Ω so that each possible degree-d polynomial P corresponds to an outcome in Ω.

(b) Let $a \in \mathbb{F}_p$. For a *fixed* $x \in \mathbb{F}_p$, compute the probability

$$\mathbb{P}[P(x) = a] .$$

Remember that the probability is over the choice of the polynomial P.

(c) Let Z be as defined above. Calculate $\mathbb{E}[Z]$.

(d) Calculate $\mathsf{Var}[Z]$.

4. **Orthonormal bases for Krylov subspaces**. **[Optional problem. No need to submit]**
Let V be a vector space and let $\varphi : V \to V$ be a linear operator. Let $v \in V$ be any vector. Then the subspace

$$\mathcal{K}_t(\varphi, v) := \text{Span}\left(\left\{v, \varphi(v), \varphi^2(v), \ldots, \varphi^{t-1}(v)\right\}\right),$$

is known as the Krylov subspace of order t defined by φ and v. In the conjugate gradient algorithm, we need to compute an orthonormal basis for the space $\mathcal{K}_t(\varphi, v)$ when V is an inner product space and φ is a self-adjoint operator with respect to this inner product. Here we will show that one can improve on the complexity of the Gram-Schmidt orthogonalization procedure when φ is a self-adjoint operator.

(a) Show that $\dim(\mathcal{K}_t(\varphi, v)) \leq t$ for all $\varphi : V \to V$ and all $v \in V$.

(b) For all $v, w \in V$, let the number of operations (arithmetic operations over $\mathbb{C}$) required to compute $\langle v, w\rangle$ and $\varphi(v)$ be at most N. Then show that one can apply the Gram-Schmidt process to the set $\left\{v, \varphi(v), \varphi^2(v), \ldots, \varphi^{t-1}(v)\right\}$ to find an orthonormal basis for $\mathcal{K}_t(\varphi, v)$ using $O(t^2 \cdot N)$ operations.

(c) When using the conjugate gradient algorithm, a complexity of $O(t^2 \cdot N)$ turns out to be too large for computing an orthonormal basis. We have $t = O(\sqrt{\kappa})$ and hence spending time $O(t^2 \cdot N)$ in computing the basis would not give us any advantage over steepest descent.

However, when φ is self-adjoint, an orthonormal basis can be computed using $O(t \cdot N)$ operations. Assume $\dim(\mathcal{K}_t(\varphi, v)) = t$ (and hence $v \neq 0$). Use induction (on i) to show that there exists a set of orthonormal vectors $\{u_0, \ldots, u_{t-1}\}$ such:

i. $\text{Span}(\{u_0, \ldots, u_{i-1}\}) = \mathcal{K}_i(\varphi, v)$ for all $i \leq t$.

ii. $\text{Span}(\{u_0, \ldots, u_{i-1}, \varphi(u_{i-1})\}) = \mathcal{K}_{i+1}(\varphi, v)$ for all $i \leq t-1$.

iii. $\langle \varphi(u_i), u_j\rangle = 0$ for all $1 \leq i \leq t-1$ and all $j \leq i-2$.

Note that to construct an orthonormal basis with the properties above, one only needs to compute $\langle u_i, \varphi(u_i)\rangle$ and $\langle u_{i-1}, \varphi(u_i)\rangle$ at every step. Thus, the basis can be constructed using $O(t \cdot N)$ operations.