Problem set 0

CSE 534 Autumn 2026

Due date: None

This problem set is intended to verify that you are up to speed on prerequisite mathematics and is neither graded nor required. However, all students enrolled are expected to be able to answer questions of this level with only minimal difficulty.

1 Complex numbers

Problem 1 (Polar Representations)**.** Consider a complex number $z \in \mathbb{C}$ such that $z = re^{i\theta}$ for $r \in \mathbb{R}^{\geq 0}$ and $\theta \in [0, 2\pi)$.

1. Show that every complex number $a + bi$ for $a, b \in \mathbb{R}$ can be expressed with a polar representation. Show that the polar representation is unique; that is $z = r'e^{i\theta'}$ if and only if $r' = r$ and $\theta' = \theta$.
2. For $z = re^{i\theta}$ and $z' = r'e^{i\theta'}$, what is the polar representation of the complex conjugate z^*? What is the polar representation of $z \cdot z'$?
3. The multiplicative inverse, denoted z^{-1}, is the unique complex number such that $z \cdot z^{-1} = 1$. What is the multiplicative inverse of $z = re^{i\theta}$, and what is the multiplicative inverse of $z = a + bi$?
4. For any natural number $n \in \mathbb{N}$, calculate the n roots (including multiplicities) of $re^{i\theta}$ and express them in terms of $\omega_n = e^{2\pi i/n}$.

Problem 2 (Geometric sums and roots of unity)**.**

1. For $z \in \mathbb{C}$ and an integer $m \geq 1$, calculate $\sum_{j=0}^{m-1} z^j$. Treat $z = 1$ separately.
2. Let $N \geq 2$ be an integer and let $\omega_N = e^{2\pi i/N}$. Show that for every integer k,

$$\sum_{j=0}^{N-1} \omega_N^{kj} = \begin{cases} N, & \text{if } N \mid k, \\ 0, & \text{if } N \nmid k. \end{cases}$$

2 Algebra review and notation

Problem 3 (Bra-ket notation)**.** Bra-ket notation is a quantum mechanics notation that is popularly used in quantum information and computation. We use $|v\rangle$ to denote a (column)-vector in $\mathbb{C}^d$. Recall that a vector is a matrix with only one column. Equivalently $|v\rangle \in \mathbb{C}^{d\times 1}$. We use $\langle v| \in \mathbb{C}^{1\times d}$ to denote the row-vector with

complex conjugate entries as that of $|v\rangle$. So if

$$|v\rangle = \begin{pmatrix} v(0) \\ v(1) \\ \vdots \\ v_(d-1) \end{pmatrix}, \text{ then } \quad \langle v| = \begin{pmatrix} v(0)^* & v(1)^* & \cdots & v(d-1)^* \end{pmatrix},$$

in terms of the entry-wise values of $|v\rangle$.

1. We use $\langle v|v\rangle$ as a short-form for $\langle v|\cdot|v\rangle$. What is the value of $\langle v|v\rangle$? What is this quantity in traditional mathematical terms? Show that this value is always real.

2. What is the matrix representation of $|v\rangle\langle v|$? What is the trace of this matrix? How could you have calculated that using the cyclicity of the trace?

3. We use $\||v\rangle\|$ to denote $\sqrt{\langle v|v\rangle}$. A vector is unit-norm if its norm equals 1. For notation, we use the following convention to describe the unit vectors pointing in each of the coordinate directions:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

   These vectors form a basis for $\mathbb{C}^d$ which is known as the *standard* or *canonical* basis. How can we express the vector $|v\rangle$ in terms of these basis vectors?

4. Similarly, we use $|i\rangle\langle i|$ as a short-form for $|i\rangle\cdot\langle i|$. What is the matrix $\sum_{i=0}^{d-1} |i\rangle\langle i|$ in traditional mathematical terms?

5. For $i \in \{0, \ldots, d-1\}$, what is the value of $\langle i|v\rangle$ for $|v\rangle$ from before? Show that

$$|v\rangle = \sum_{i=0}^{d-1} \langle i|v\rangle\, |i\rangle\,.$$

   Hint: Use the decomposition of $\mathbb{I}$ from the previous question and use that $\langle i|v\rangle$ is a scalar.

6. Let $|v\rangle$ and $|w\rangle$ be unit vectors. Let $M = |w\rangle\langle v|$. What is the value of $M|v\rangle$? Let $|v^\perp\rangle$ be a vector such that $\langle v|v^\perp\rangle = 0$. What is $M|v^\perp\rangle$?

7. Let M be a square matrix $\in \mathbb{C}^{d\times d}$ with columns $|v_0\rangle, |v_1\rangle, \ldots, |v_{d-1}\rangle$. Show that

$$M = \sum_{i=0}^{d-1} |v_i\rangle\langle i| .$$

8. Let M be a matrix in $\mathbb{C}^{d\times d}$ and $|v\rangle$ a vector in $\mathbb{C}^d$. Argue that the $\langle v| M^\dagger$ is the conjugate transpose of $M|v\rangle$.

If that went well, you should be able to start using bra-ket notation. It will become more natural over time!

Problem 4 (Bases for vector spaces)**.** A set $V \subset \mathbb{C}^d$ is a subspace if it is closed under scalar multiplication and addition. A basis B for a vector space is a collection of vectors such that every vector can be expressed as a linear combination of vectors from B and B is of minimal cardinality.

1. Show that all bases for a vector space $V \subset \mathbb{C}^d$ have the same cardinality, which is an integer between 0 and d.
2. Show that $|v_0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ and $|v_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$ form a basis for $\mathbb{C}^2$. Express the vectors $|0\rangle$ and $|1\rangle$ (see definitions above) in terms of this basis. The vectors $|v_0\rangle$ and $|v_1\rangle$ are used so much in quantum computation that they have special names: $|+\rangle$ and $|-\rangle$.
3. Express the vectors $|0\rangle$ and $|1\rangle$ in terms of $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$ and $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$.

A basis is called orthonormal if all the vectors in the basis are orthogonal to each other and of unit norm. To define orthogonality and norm, we will need the next problem:

Problem 5 (Inner-product spaces)**.** Consider a vector space V with a function $f : V \times V \to \mathbb{C}$ satisfying the following properties: For all vectors $u, v, w \in V$,

- (linearity) for all $\alpha, \beta \in \mathbb{C}$, $f(u, \alpha v + \beta w) = \alpha f(u, v) + \beta f(u, w)$.
- (complex conjugate symmetry) $f(u, v) = f(v, u)^*$.
- (positivity) $f(u, u) \in \mathbb{R}^+$ and $f(u, u) = 0$ iff $u = 0$.

Such a vector space is called an inner product space. When considering finite-dimensional vector spaces, inner product spaces are *equivalent* to Hilbert spaces.

1. Show that $f(\alpha u, v) = \alpha^* f(u, v)$.
2. Show that the bilinear form given by $f(|u\rangle, |v\rangle) = \langle u|v\rangle$ for $|u\rangle, |v\rangle \in \mathbb{C}^d$ makes $\mathbb{C}^d$ an inner product space.

3. In a lot of mathematical notation, the function f is often expressed as a bilinear form: $\langle \cdot, \cdot \rangle \stackrel{\text{def}}{=} f(\cdot, \cdot)$. The bra-ket notation was adopted in part because it matches this. We previously defined the norm as $\||v\rangle\| = \sqrt{\langle v|v\rangle}$. Show that the function $\|\cdot\| : \mathbb{C}^d \to \mathbb{R}^+$ defined from the inner product yields a metric which is a function satisfying linearity, positivity, and the triangle inequality.

4. Recall that in a metric space, by the Pythagorean theorem, two unit vectors $|u\rangle$ and $|v\rangle$ are orthogonal if $\||u\rangle - |v\rangle\| = \sqrt{2}$. Show that this is true iff $\langle u|v\rangle = 0$.

5. Generalize to show that if $|\langle u|v\rangle| \leq \epsilon$, then

$$\||u\rangle - |v\rangle\|^2 \geq 2(1 - \epsilon).$$

   This says that when the inner product is small, then the two vectors are far from each other.

6. Show the converse is false. Find vectors such that $|\langle u|v\rangle| = 1$ but they are maximally far apart.

7. Show that if $|\langle u|v\rangle| \geq 1 - \epsilon$, then there exists an angle $\theta \in [0, 2\pi)$ such that

$$\left\| |u\rangle - e^{i\theta} |v\rangle \right\| \leq \sqrt{2\epsilon}.$$

   This shows that a large inner product implies that the two vectors are close "up to phase".

Problem 6 (Linear transformations)**.** Recall/show that over a vector space $V \subseteq \mathbb{C}^d$, any linear transformation $T : V \to V$ has a matrix representation such that $T(|v\rangle) = M_T |v\rangle$. For this reason, we often use the same symbol to represent the linear transform and its matrix representation. For a bilinear form $\langle \cdot, \cdot \rangle$ defining an inner product space, the adjoint of a linear transform T is the transformation $T^\dagger$ such that

$$\langle T^\dagger u, v\rangle = \langle u, Tv\rangle.$$

1. Show that the adjoint of a linear transform with matrix representation T for the bilinear form $\langle \cdot | \cdot \rangle$ is defined by the conjugate transpose.

2. A matrix $H \in \mathbb{C}^{d \times d}$ is Hermitian if $H^\dagger = H$ where $H^\dagger$ is the conjugate transpose.

   (a) Show that the diagonal coordinates of H must be real.

   (b) Show that the eigenvalues of H must be real.

   Hint: assume $|v\rangle$ is a unit eigenvector of H of eigenvalue $\lambda \in \mathbb{C}$. Argue that then $\lambda = \lambda^*$.

   (c) Let $|v\rangle$ be a unit eigenvector of eigenvalue $\lambda \in \mathbb{R}$. Let $H' = H - \lambda |v\rangle\langle v|$. Show that $H' |v\rangle = 0$. Next, let $|w\rangle$ be a vector orthogonal to $|v\rangle$. Show that $H' |w\rangle = H |w\rangle$.

   (d) Let $\Pi = \mathbb{I} - |\lambda\rangle\langle\lambda|$. Recall that a matrix is a projection if it equals its square, or equivalently, its eigenvalues are either 1 or 0. Show that Π is a projection — i.e. $\Pi^2 = \Pi$. Show that $H' = \Pi H \Pi$.

(e) Use this and the Gram-Schmidt process to show that there exist eigenvalues $\lambda_0, \ldots, \lambda_{d-1} \in \mathbb{R}$ and an orthonormal set of eigenvectors $|v_0\rangle, \ldots, |v_{d-1}\rangle$ such that

$$H = \sum_{i=0}^{d-1} \lambda_i |v_i\rangle\langle v_i| .$$

3. A matrix $U \in \mathbb{C}^{d\times d}$ is unitary if $U^\dagger U = \mathbb{I}$. Show that the following are equivalent by proving that each implies the next and the last implies the first.

   - U is unitary.
   - U maps an orthonormal basis to an orthonormal basis.
     What is the bilinear form between $U|u\rangle$ and $U|v\rangle$?
     Hint: If $|u\rangle$ and $|v\rangle$ are orthogonal, then the bilinear form $\langle 0|0\rangle = 0$.
   - U maps any unit vector to another unit vector.

Problem 7 (Vectorization and the Hilbert–Schmidt inner product)**.** Let $m, n \geq 1$ be integers. For a matrix $A = \sum_{i,j} A_{ij} |i\rangle\langle j| \in \mathbb{C}^{m\times n}$, define its *vectorization* $|\mathrm{vec}\, A\rangle \in \mathbb{C}^m \otimes \mathbb{C}^n$ by

$$|\mathrm{vec}\, A\rangle \stackrel{\text{def}}{=} \sum_{i,j} A_{ij} |i\rangle |j\rangle ,$$

where $0 \leq i < m$ and $0 \leq j < n$.

1. Show that $A \mapsto |\mathrm{vec}\, A\rangle$ is a linear bijection between $\mathbb{C}^{m\times n}$ and $\mathbb{C}^m \otimes \mathbb{C}^n$ by explicitly identifying the linear bijection.

2. For $A, B \in \mathbb{C}^{m\times n}$, show that

   $$\langle \mathrm{vec}\, A | \mathrm{vec}\, B\rangle = \mathrm{tr}\big(A^\dagger B\big),$$

   where the left-hand side is the usual inner product on $\mathbb{C}^m \otimes \mathbb{C}^n$.

3. Prove that $\langle A, B\rangle_{\mathrm{HS}} \stackrel{\text{def}}{=} \mathrm{tr}\big(A^\dagger B\big)$ is a well-defined inner product on $\mathbb{C}^{m\times n}$. It is called the *Hilbert–Schmidt inner product.*

4. Suppose we change the ordering of the entries in the vectorization, using the same ordering for both A and B. Does this change the inner product of the vectorizations? Explain your answer.

3 Probability theory

Problem 8 (Random fingerprints)**.** Let $S \subseteq \{0,1\}^n$ be a fixed set with $|S| \geq 2$. We want to assign each string a short *fingerprint* so that no two strings in S have the same fingerprint. Choose $a_1, \ldots, a_k \in \{0,1\}^n$

uniformly and independently, and define

$$h(x) = (a_1 \cdot x, \dots, a_k \cdot x) \in \{0,1\}^k, \qquad a \cdot x \stackrel{\text{def}}{=} \sum_{j=1}^{n} a_j x_j \pmod 2.$$

1. For distinct $x, y \in S$ and uniform $a \in \{0,1\}^n$, calculate $\mathbf{Pr}_a[a \cdot x = a \cdot y]$. Deduce the probability that $h(x) = h(y)$.
2. Use the union bound to bound the probability that h fails to be injective on S. For $\delta \in (0,1)$, give an explicit sufficient choice of k that makes this probability at most δ. Must the collision events for different pairs be independent for your argument to work? Are they always independent? Justify your answers.
3. Conclude that there exists a choice of $k = \lceil 2 \log_2 |S| \rceil$ parity tests whose fingerprints distinguish every pair of strings in S simultaneously.
4. Show that any injective function $g : S \to \{0,1\}^k$, whether or not it uses parity tests, requires $k \geq \lceil \log_2 |S| \rceil$. When $k < n$, can a single choice of h work for every $|S|$-element subset of $\{0,1\}^n$ simultaneously? Explain your answer.

Problem 9 (Repeated trials and expected running time)**.** An experiment succeeds with probability $p \in (0,1)$, independently each time it is performed. Let T be the number of trials up to and including the first success.

1. Calculate $\mathbf{Pr}[T > t]$ for every integer $t \geq 0$, and calculate $\mathbf{Pr}[T = t]$ for every integer $t \geq 1$.
2. Calculate $\mathbf{E}[T]$.
3. For $\delta \in (0,1)$, give a sufficient number of trials to obtain at least one success with probability at least $1 - \delta$. Express your bound in terms of p and δ.

   Hint: You may use $1 - p \leq e^{-p}$.
4. Suppose $p = n^{-c}$, where $n \geq 2$ and $c > 0$ is a fixed constant. How do the expected number of trials and your bound from the previous part depend on n and δ?

Problem 10 (Estimating a mean: median of means)**.** Let X be a real-valued random variable with unknown mean $\mu = \mathbf{E}[X]$ and variance $\mathbf{Var}[X] \leq \sigma^2$, where $\sigma > 0$ is a known bound. Given $0 < \epsilon \leq \sigma$ and $\delta \in (0, 1/2)$, our goal is to estimate μ to additive error ϵ with failure probability at most δ.

Draw kb independent copies $X_{j,\ell}$ of X, arranged into k disjoint groups of b samples, where k is odd. Define the group averages and their median by

$$Y_j = \frac{1}{b} \sum_{\ell=1}^{b} X_{j,\ell}, \qquad \widehat{\mu} = \text{median}(Y_1, \dots, Y_k).$$

Here the median is the middle value after sorting the k group averages. You may use Chebyshev's inequality without proof: $\mathbf{Pr}[|Z - \mathbf{E}[Z]| \geq t] \leq \mathbf{Var}[Z]/t^2$ for $t > 0$.

1. Calculate $\mathbf{E}[Y_j]$ and bound $\mathbf{Var}[Y_j]$. Show that if $b \geq 16\sigma^2/\epsilon^2$, then $\mathbf{Pr}[|Y_j - \mu| \geq \epsilon] \leq 1/16$.

2. Call group j *bad* if $|Y_j - \mu| \geq \epsilon$. Show that $|\widehat{\mu} - \mu| \geq \epsilon$ implies that at least $(k+1)/2$ groups are bad. Using independence and the union bound, prove that

   $$\mathbf{Pr}[|\widehat{\mu} - \mu| \geq \epsilon] \leq 2^{-k}.$$

3. Give explicit choices of b and odd k that achieve failure probability at most δ. Show that the total number of samples is

   $$O\left(\frac{\sigma^2}{\epsilon^2} \log \frac{1}{\delta}\right).$$

   What sample bound would Chebyshev's inequality alone give if we used a single average instead? Compare the dependence on δ.

Problem 11 (Fixing the randomness: $\mathsf{BPP} \subseteq \mathsf{P/poly}$)**.** A language $\mathcal{L} \subseteq \{0,1\}^*$ belongs to BPP if there is a randomized polynomial-time algorithm A such that, for every input x,

$$\Pr_r[A(x;r) = \mathcal{L}(x)] \geq \frac{2}{3},$$

where $\mathcal{L}(x)$ is 1 if $x \in \mathcal{L}$ and 0 otherwise. On inputs of length n, the random seed r is uniform in $\{0,1\}^{q(n)}$ for some polynomial q. An algorithm using fewer random bits can be padded with unused bits. A language belongs to $\mathsf{P/poly}$ if there is a family of deterministic Boolean circuits $\{C_n\}_{n \geq 1}$, each of size polynomial in n, such that $C_n(x) = \mathcal{L}(x)$ for every $x \in \{0,1\}^n$. No efficient procedure for constructing C_n from n is required.

Assume $\mathcal{L} \in \mathsf{BPP}$. We will prove that $\mathcal{L} \in \mathsf{P/poly}$.

1. Using the Chernoff bound, construct a randomized polynomial-time algorithm B such that, for every $x \in \{0,1\}^n$,

   $$\Pr_R[B(x;R) \neq \mathcal{L}(x)] \leq 2^{-(n+1)}.$$

   Bound the number of repetitions and the total number of random bits used.

2. Fix an input length n. Prove that there exists a *single* random seed R_n such that

   $$B(x;R_n) = \mathcal{L}(x) \qquad \text{for every } x \in \{0,1\}^n.$$

The same seed must work for every input of length n.

3. Show that hardwiring R_n yields a deterministic Boolean circuit C_n of size polynomial in n. Conclude that $\mathsf{BPP} \subseteq \mathsf{P/poly}$.

4. Why does this argument not prove that $\mathsf{BPP} = \mathsf{P}$?