Homework 4

CS 70, Summer 2024

Due by Sunday, July 21$^{\text{st}}$ at 11:59 PM

This content is protected and may not be shared, uploaded, or distributed.

Instructions. Start each problem on a separate page. The subparts of each problem can be on the same page. Every answer should contain a calculation or reasoning. Your answers should be clear, organized, and legible—your final submission should not include scratch work or failed attempts. You must always commit to a final answer; if multiple answers are provided, the most incorrect one will be graded. You may leave all algebraic expressions unsimplified, but you must simplify any infinite sums or integrals unless otherwise stated.

If you are completing the homework using LaTeX, you may use the templates. Homeworks must be submitted through Gradescope. See the end of the homework for submission instructions.

Sundry. Before you start writing your final homework submission, state briefly how you worked on it (e.g., if you went to office hours, how frequently you worked on it, etc.). If you worked on the assignment in a group with other students, list their names and email addresses.

1 Polynomial Proofs

Recall that we say that a function p is a *polynomial* if there exists constants $c_0, \ldots, c_d$, called *coefficients*, and some natural number $d \in \mathbb{N}$ such that

$$p(x) = c_d x^d + \ldots + c_1 x + c_0 = \sum_{k=0}^{d} c_k x^k.$$

Here, x is referred to as the *variable* of the polynomial. The "type" of the variable determines what kind of polynomial p is: real, complex, modular, matrix, etc.

The *degree* of a polynomial is the exponent of the highest power of its variable with a nonzero coefficient. The zero polynomial $p = 0$ has no defined degree.

(a) Prove that for any two polynomials f and g, the function $f + g$ is also a polynomial, and if $f + g \neq 0$, then

$$\deg(f + g) \leq \max(\deg f, \deg g).$$

(b) Prove that for any two polynomials f and g, the function $f \cdot g$ is also a polynomial and has degree $\deg f \cdot g = \deg f + \deg g$.

(c) Prove the *division algorithm* for polynomials. That is, for any polynomial a and any nonzero polynomial b, there exist polynomials q and r which are unique up to scaling by constants such that $a = bq + r$ and $\deg r < \deg b$.

We call r the *remainder* of a when dividing by b, and write $r = a \bmod b$.

(d) Recall that we say that a polynomial b *divides* another polynomial a if the remainder polynomial from the division algorithm is zero; that is, if $a = bq$ for some polynomial q. We write $b \mid a$.

We further define the greatest common divisor $\gcd(a, b)$ of two polynomials a and b to be the highest degree polynomial which divides both of them.

Prove *Bezout's identity* for polynomials. That is, prove that for any two polynomials a and b such that $d = \gcd(a, b)$, there exist two polynomials y and z such that

$$ay + bz = d.$$

2 The Polynomial Arithmetic

We have seen in **Question 1** that we can define remainders when dividing polynomials by other polynomials in the same way we can define remainders when dividing integers by other integers.

In this question, we will investigate the polynomial arithmetic, which is the arithmetic formed by equating all polynomials which share the same remainder when divided by some modulus polynomial. We will see that this arithmetic is in many ways the same as the modular arithmetic which we have been studying in the past few weeks of the course.

For any two polynomials a and b, we say that $a \equiv b \pmod{m}$ if $m \mid (a - b)$. We say that a and b are *congruent modulo m*.

(a) Prove that for any two polynomials a, b and nonzero polynomial m, the following are logically equivalent.

(1) $a \equiv b \pmod{m}$.

(2) $a \bmod m = b \bmod m$.

(3) There exists some polynomial k such that $a = km + b$.

(b) In this part, we'll try to understand a little better what exactly is going on with these polynomial moduli.

Let p be a prime, let a and b be any polynomials, and let m be a nonzero polynomial, all over the finite field $\mathbb{F}_p$.

Prove that

$$a \equiv b \pmod{m} \iff a(x) \equiv b(x) \pmod{m(x)} \quad \text{for each } x \in \mathbb{F}_p.$$

This shows that we can think of a congruence with a polynomial modulus as a set of congruences: one for each x. While this intuition only works when we're working with polynomials over finite fields, it can be useful in thinking about what these equations mean.

(c) Let a, b, c, d be any four polynomials and m be a nonzero polynomial such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Prove that

$$a + c \equiv b + d \pmod{m} \qquad \text{and} \qquad ac \equiv bd \pmod{m}.$$

(d) For any polynomial a and nonzero polynomial m, we say that y is *an inverse of a modulo m* if $ay \equiv 1 \pmod{m}$.

Prove that the inverse of a exists and is unique modulo m and scaling by constants if $\gcd(a, m) = 1$.

(e) Solve the polynomial congruence

$$p(x)x^3 \equiv x + 1 \pmod{x^2 + 1}.$$

for all solutions p.

3 Counting, Counting, Counting

For each of the following parts, count the number of elements in the provided set. Justify each answer with 3 – 4 sentences.

(a) The permutations of $\{1, \ldots, n\}$ with at least $k \in \{0, \ldots, n\}$ fixed points.

(A *permutation* is a bijection from a set to itself. A *fixed point* of a function f is a value x such that $f(x) = x$.)

(b) The integer solutions to $x_1 + x_2 + x_3 + x_4 = n$ for some natural number n, where $x_1 \geq -3$, $x_2, x_3 \geq 0$ and $x_4 \geq 3$.

For example, for $n = 6$, we consider $x_1 = 0, x_2 = 0, x_3 = 3, x_4 = 3$ and $x_1 = 3, x_2 = 0, x_3 = 0, x_4 = 3$ as two distinct solutions.

(c) The bridge hands from a standard deck of cards which have at least one quad.

(A *standard deck* consists of 52 cards, 26 of which are red and 26 of which are black. Of the red cards, 13 are diamonds and 13 are hearts, while of the black cards, 13 are clubs and 13 are spades. The four categories of diamonds, hearts, clubs, and spades are called *suits*. Each of the 13 cards in a suit have a *rank*: 2, 3, 4, 5, 6, 7, 8, 9, 10, J, K, Q, A. There are 4 cards of each rank in a deck: one for each suit.)

(A *bridge hand* consists of thirteen cards drawn without replacement.)

(A *quad* is four cards from the same rank.)

(d) The sequences of $k \geq n$ draws from $\{1, \ldots, n\}$ with replacement which include each of the n elements at least once.

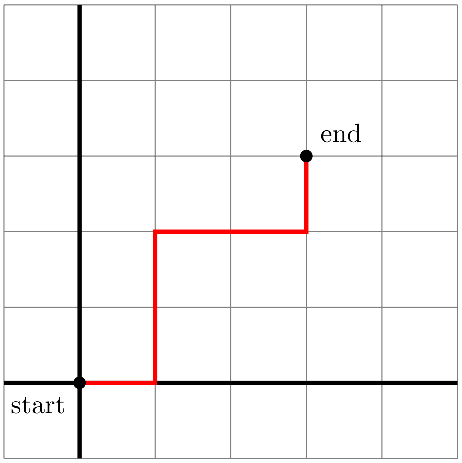
(e) The permutations of the cards of a standard deck in which an ace never appears in the first $k \leq 48$ cards.

4 The Catalan Numbers

In this question, we will investigate the *Catalan numbers*, which appear frequently in counting problems for objects with recursive structures.

Consider an ant, Antony, walking on the the infinite lattice $\mathbb{Z} \times \mathbb{Z}$. For some $n \in \mathbb{N}$, Antony starts at the origin $(0, 0)$ and walks to the point (n, n). Antony walks in steps, wherein each step Antony traverses a single edge of the grid. Antony can only walk right or up; that is, Antony will never "go backwards."

Below is an example with $n = 3$. One possible path which Antony could take is drawn in red.

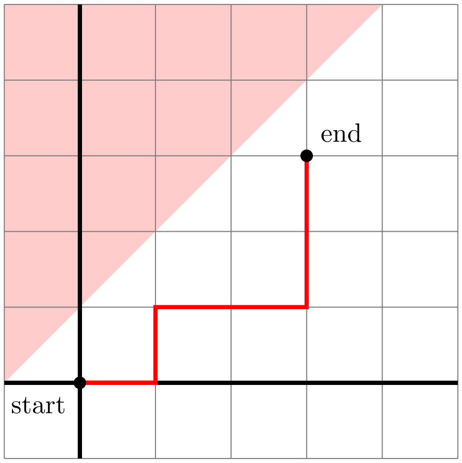


(a) Explain why the length of any path Antony takes is $2n$ steps.

(b) Count the number of paths Antony could take.

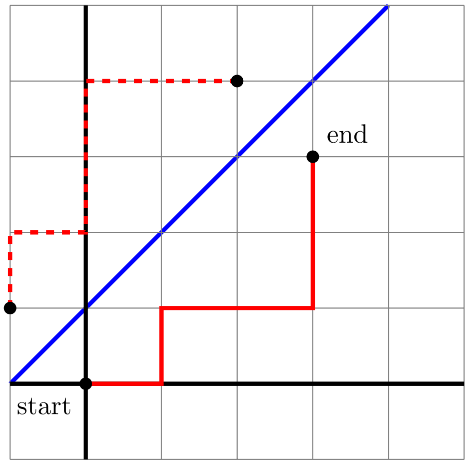
(c) Now suppose that the grid points (x, y) such that $y \geq x + 1$ are on fire, so Antony cannot take paths which touch such points.

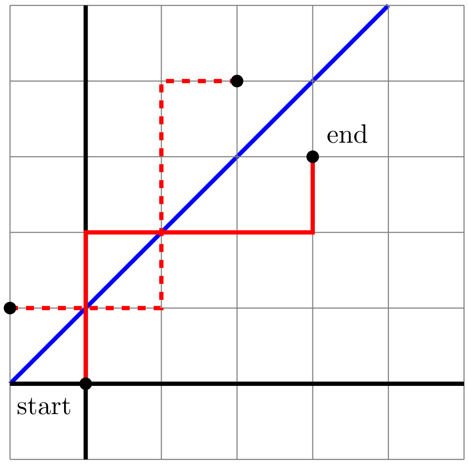
Below is an example with $n = 3$. The region which Antony can no longer visit is shaded in red. One possible path which Antony could take is drawn in red.



Consider the function f which takes a path $P \in (\mathbb{Z} \times \mathbb{Z})^{2n}$ and reflects it across the line $y = x + 1$.

Below are two examples of this function. The original paths are drawn solid, while the reflected path are drawn dashed.

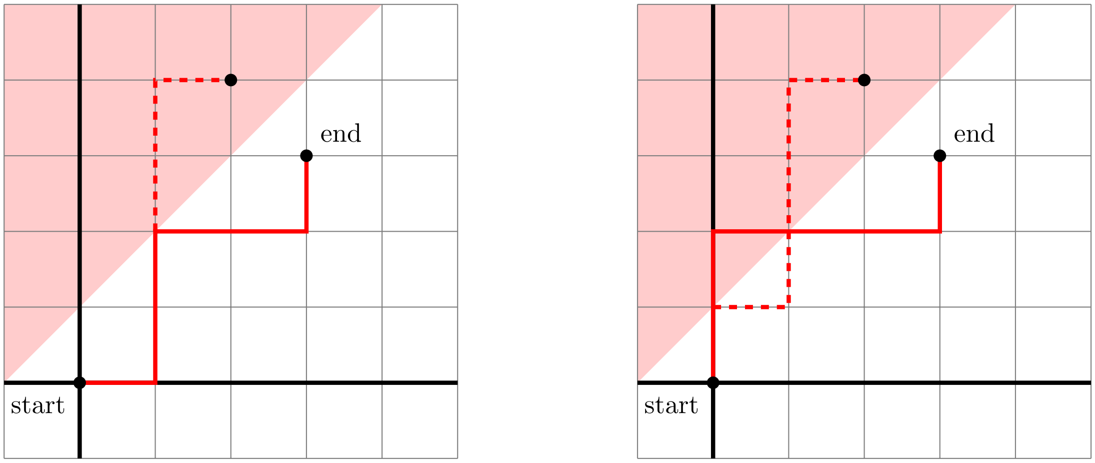




Write down a formula for this function in terms of some input path $P = ((x_0, y_0), (x_1, y_1), \ldots, (x_{2n}, y_{2n})) \in (\mathbb{Z} \times \mathbb{Z})^{2n}$.

(d) Consider any "fiery path" which passes through the fire. Such a fiery path must hit the line $y = x + 1$ at some point. We form a new path through the *reflection process* by reflecting any such fiery path after it hits the line $y = x + 1$ along the line $y = x + 1$.

Below are two example of the reflection process. The new path consists of the portion of the fiery path until it hits the fire along with the reflected portion of the fiery path, which is drawn dashed.



Explain why any path created by applying the reflection process to a fiery path results in a path which starts at $(0, 0)$ and goes to $(n - 1, n + 1)$.

(e) Argue that applying the reflection process to any two distinct fiery paths yields two distinct paths from $(0, 0)$ to $(n - 1, n + 1)$.

(f) Argue that any paths from $(0, 0)$ to $(n - 1, n + 1)$ can be formed by applying the reflection process to a fiery path.

(g) Use parts **(d)**, **(e)**, and **(e)** to count the number of fiery paths.

(h) Count the number of paths which Antony could take which do not pass through the fire. This is known as the *Catalan number* C_n.

(i) Provide a combinatorial proof of the following identity.

$$C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}.$$

Conventions. In this class, you may assume the following unless otherwise stated.

- A coin is equally likely to land heads or tails, regardless of the results of other tosses.
- A die is equally likely to show any of its six sides, regardless of the results of other rolls.
- Choosing at random means that each element in the set of choices is equally likely.
- A standard deck consists of 52 cards, 26 of which are red and 26 of which are black. Of the red cards, 13 are diamonds and 13 are hearts, while of the black cards, 13 are clubs and 13 are spades. The four categories of diamonds, hearts, clubs, and spades are called suits. Each of the 13 cards in a suit have a rank: 2, 3, 4, 5, 6, 7, 8, 9, 10, J, K, Q, A. There are 4 cards of each rank in a deck: one for each suit.

Otherwise, **anything not stated cannot be assumed**.

Instructions. Now that we have moved on to probability, our answers will become much more numerical in nature. You may leave all algebraic expressions unsimplified, but you must simplify all infinite sums and all integrals unless otherwise stated. Every answer should contain a calculation or reasoning. Reasoning can be brief and abbreviated, e.g., ”multiplication rule” or ”mutually exclusive.”

5 Earthquakes

Seismologists are considering whether an earthquake will happen within the next year in three different regions. Let N_1, N_2, and N_3 be the events that there is no earthquake within the next year in each of three different seismically active regions.

(a) Let N be the event that none of the three regions have an earthquake within the next year. If it is possible, determine whether $\mathrm{P}(N) < \mathrm{P}(N_1)$, $\mathrm{P}(N) = \mathrm{P}(N_1)$, or $\mathrm{P}(N) > \mathrm{P}(N_1)$. If it is not possible, explain why.

(b) The seismologists have determined that

$$\mathrm{P}(N_1) = 0.93 \qquad \mathrm{P}(N_2) = 0.95 \qquad \mathrm{P}(N_3) = 0.99.$$

If it is possible, find the chance that at least one of the three regions doesn't have an earthquake within the next year. Otherwise, provide the best possible bounds.

(c) If it is possible, find the chance that none of the three regions have an earthquake within the next year. Otherwise, provide the best possible bounds.

(d) Further suppose that the seismologists have determined that the seismic activity in the first region has a large effect on the seismic activity in the second region. In particular, they have found that $\mathrm{P}(N_2 \mid N_1) = 0.99$.

If it is possible, find the chance that there is an earthquake in the first region within the next year, but not in the second region. Otherwise, provide the best possible bounds.

6 Balls in Bins

We have seen that the balls-in-bins model is a general model with myriad applications. In particular, throwing balls independently at random into bins models any sort of experiment with independent trials which have equally likely outcomes.

For each of the following problems, consider how the setting is like throwing some number of balls into some number of bins. Thinking about where the balls must land for the event to occur will help you reach the answer.

(a) A bored probabilist sits at their computer and types letters at random. For each keystroke, the probabilist types one of the 26 letters, independently of the other letters which they type. The probabilist types out 11 such letters.

Find the chance that the typed letters can be arranged to form the word "PROBABILITY."

(b) A group of 6 students attend office hours and each asks a question about one of the 6 problems on this homework, independently of the other students. Find the chance that they all ask about different problems.

(c) A fair six-sided die is rolled n times. Find the chance that the face with six spots is never rolled.

(d) A fair six-sided die is rolled $n \geq 6$ times. Find the chance that every face is seen.

Submission. Homeworks must be submitted through Gradescope. If you are completing your homeworks on paper, please scan the pages of your homework into a PDF using any scanner or phone application such as CamScanner. **It is your responsibility to ensure that all the work on the scanned pages is legible.**

Once you upload your submission to the Gradescope assignment, you will be prompted to select pages. **It is your responsibility to correctly select the pages of your homework corresponding to each question.** If you are having difficulties scanning, uploading, or submitting your homework, post a follow-up on the main thread corresponding to this homework on Ed.