Homework 4

CS 70, Summer 2024

Due by Sunday, July 21th at 11:59 PM

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

1 Polynomial Proofs

(a) Let $d_f = \deg f$ and $d_g = \deg g$.

By definition, there are coefficients $a_0, \ldots, a_{d_f}$ and $b_0, \ldots, b_{d_g}$ such that

$$f(x) = \sum_{k=0}^{d_f} a_k x^k \qquad \text{and} \qquad g(x) = \sum_{k=0}^{d_g} b_k x^k \qquad \text{for all } x.$$

(1) Suppose that $d_f \geq d_g$.

Then for any x,

$$\begin{aligned} f(x) + g(x) &= \sum_{k=0}^{d_f} a_k x^k + \sum_{k=0}^{d_g} b_k x^k \\ &= \sum_{k=0}^{d_g} a_k x^k + \sum_{k=d_g+1}^{d_f} a_k x^k + \sum_{k=0}^{d_g} b_k x^k \\ &= \sum_{k=0}^{d_g} (a_k + b_k) x^k + \sum_{k=d_g+1}^{d_f} a_k x^k \\ &= \sum_{k=0}^{d_f} c_k x_k, \end{aligned}$$

where

$$c_k = \begin{cases} a_k + b_k & \text{if } k \leq d_g \\ a_k & \text{otherwise.} \end{cases}$$

So $f + g$ is indeed a polynomial. Additionally, we have that

$$\deg(f+g) \leq d_f = \deg f = \max(\deg f, \deg g,$$

where $\deg f = \max(\deg f, \deg g)$ since $d_f \geq d_g$.

Note that if $d_f > d_g$, then this is an equality, since the highest power of the variable in $f + g$ is $a_{d_f} x^{d_f}$. However, if $d_f = d_g$, it is possible that $b_{d_g} = -a_{d_f}$; thus, in $f + g$, we have that $(a_{d_f} + b_{d_f})x^{d_f} = 0$, in which case the degree is smaller than d_f.

(2) Now instead suppose $d_g > d_f$.

Then the same algebra shows that for any x,

$$f(x) + g(x) = \sum_{k=0}^{d_g} c_k x^k$$

where

$$c_k = \begin{cases} a_k + b_k & \text{if } k \leq d_f \\ b_k & \text{otherwise.} \end{cases}$$

In this case,

$$\deg(f+g) = d_g = \deg g = \max(\deg f, \deg g),$$

where $\deg g = \max(\deg f, \deg g)$ since $d_g > d_f$.

In either case, we have that $f + g$ is a polynomial and that $\deg(f+g) \leq \max(\deg f, \deg g)$, as desired.

(b) Let $d_f = \deg f$ and $d_g = \deg g$. By definition, there are coefficients $a_0, \ldots, a_{d_f}$ and $b_0, \ldots, b_{d_g}$ such that

$$f(x) = \sum_{k=0}^{d_f} a_k x^k \qquad \text{and} \qquad g(x) = \sum_{k=0}^{d_g} b_k x^k \qquad \text{for all } x.$$

We prove this by induction on the degree of f, d_f.

Base case. $d_f = 0$. Then $f = a_0$ and for any x,

$$f(x) \cdot g(x) = a_0 \sum_{k=0}^{d_g} b_k x^k = \sum_{k=0}^{d_g} a_0 b_k x^k = \sum_{k=0}^{d_g} c_k x^k$$

where $c_k = a_0 b_k$. So $f \cdot g$ is a polynomial.

Furthermore, suppose $f \cdot g \neq 0$. Then $g \neq 0$, and since $\deg g = d_g$, we must have that $b_{d_g} \neq 0$. Also, $f = a_0 \neq 0$. Then $a_0 b_{d_g} \neq 0$ and hence the highest power of the variable in $f \cdot g$ is d_g, so $\deg f \cdot g = \deg g = \deg g + 0$, as desired.

Induction case.

Induction hypothesis. Suppose that for any polynomial f with $\deg f \leq n$ and any polynomial g, $f \cdot g$ is a polynomial, and if $f \cdot g \neq 0$, then $\deg f \cdot g = \deg f + \deg g$.

Induction step. Consider $d_f = n + 1$. Then for any x,

$$\begin{aligned} f(x)g(x) &= \left(\sum_{k=0}^{n+1} a_k x^k \right) g(x) \\ &= \left(a_{n+1} x^{n+1} + \sum_{k=0}^{n} a_k x^k \right) g(x) \\ &= a_{n+1} x^{n+1} g(x) + f'(x) g(x), \end{aligned}$$

where

$$f'(x) = \sum_{k=0}^{n} a_k x^k$$

is a polynomial with $\deg f' \leq n$. By the induction hypothesis, $f' \cdot g$ is some polynomial.

Moreover, for any x

$$a_{n+1} x^{n+1} g(x) = a_{n+1} x^{n+1} \sum_{k=0}^{d_g} b_k x^k = \sum_{k=0}^{d_g} a_{n+1} b_k x^{k+n+1} = \sum_{j=n+1}^{d_g+n+1} c_j x^j,$$

where $c_j = a_{n+1} b_{j-(n+1)}$ for each $j \in \{n+1, \ldots, d_g + n + 1\}$. This is a polynomial.

Therefore

$$f(x)g(x) = \sum_{j=n+1}^{d_g+n+1} c_j x^j + f'(x) g(x)$$

is a polynomial by part **(a)** since it is the sum of two polynomials.

Further suppose that $f \cdot g \neq 0$. Then, since f has degree $n + 1$, $a_{n+1} \neq 0$; likewise, since g has degree d_g, $b_{d_g} \neq 0$. Then, since $a_{n+1} b_{d_g} \neq 0$, the highest power of the variable in $f \cdot g$ is $d_g + n + 1$. Thus we have that $\deg f \cdot g = d_g + n + 1 = \deg f + \deg g$, as desired.

By the principle of mathematical induction, we have shown that $f \cdot g$ is a polynomial, and if $f \cdot g \neq 0$, then $\deg f \cdot g = \deg f + \deg g$.

(c) We mimic the proof by well-ordering of the division algorithm for the integers. Consider the set

$$S = \{\deg(a - bk) : k \text{ is a polynomial}\}.$$

We claim that $S \neq \varnothing$. To see this, observe that for $k = 0$, $a - bk = a$. So $\deg a \in S$.

Let r be the polynomial such that $\deg r \in S$ is the smallest element of S.

Since $r \in S$, we have that $r = a - bq$ for some polynomial q. We claim that $\deg r < \deg b$. Suppose for contradiction that $\deg r \geq \deg b$. Then for $j = \deg b$ and $\ell \geq 0$, we have that

$$r(x) = \sum_{i=0}^{j+\ell} c_i x^i = c_{j+\ell} x^{j+\ell} + \sum_{i=0}^{j+\ell-1} c_i x^i,$$
$$b(x) = \sum_{i=0}^{j} d_i x^i = d_j x^j + \sum_{i=0}^{j-1} d_i x^i.$$

Let

$$r'(x) = \sum_{i=0}^{j+\ell-1} c_i x^i \qquad \text{and} \qquad b'(x) = \sum_{i=0}^{j-1} d_i x^i \qquad \text{for all } x,$$

So

$$r(x) = c_{j+\ell} x^{j+\ell} + r'(x) \qquad \text{and} \qquad b(x) = d_j x^j + b'(x) \qquad \text{for all } x,$$

where $\deg r' < j + \ell$ and $\deg b' < j$.

Our goal is to construct a new polynomial s such that $\deg s \in S$ and $\deg s < \deg r$. To this end, once again mimicking the proof of the division algorithm in Note 7, consider the polynomial

$$s = r - \frac{c_{j+\ell}}{d_j} x^\ell b.$$

Then, for any x,

$$\begin{aligned} s(x) &= c_{j+\ell} x^{j+\ell} + r'(x) - \left(\frac{c_{j+\ell}}{d_j} x^\ell \cdot d_j x^j + \frac{c_{j+\ell}}{d_j} x^\ell \cdot b'(x) \right) \\ &= c_{j+\ell} x^{j+\ell} + r'(x) - c_{j+\ell} x^{j+\ell} - \frac{c_{j+\ell}}{d_j} x^\ell \cdot b'(x) \\ &= r'(x) + \frac{c_{j+\ell}}{d_j} x^\ell \cdot (-b'(x)). \end{aligned}$$

Using the polynomial rules from part **(a)**, we have that

$$\deg s \leq \max \Big(\deg r', \deg \left(x^\ell \cdot (-b') \right) \Big).$$

We know that $\deg r' < j + \ell$ by construction. Moreover, since

$$-b'(x) = \sum_{i=0}^{j-1} (-d_i) x^i \qquad \text{for all } x,$$

we have that $\deg(-b') = \deg b'$. Therefore $\deg \left(x^\ell (-b') \right) = \deg x^\ell + \deg(-b') = \deg x^\ell + \deg b < j + \ell$.

Therefore

$$\deg s \leq \max \Big(\deg r', \deg \left(x^\ell \cdot (-b') \right) \Big) < j + \ell = \deg r,$$

so $\deg s < \deg r$. Moreover, since $r = a - bq$,

$$s = r - \frac{c_{j+\ell}}{d_j} x^\ell b = (a - bq) - \frac{c_{j+\ell}}{d_j} x^\ell b = a - b \left(\frac{c_{j+\ell}}{d_j} x^\ell + q \right).$$

So $\deg s \in S$. But this is contradiction, since $\deg r \in S$ is the least degree in S. So our assumption that $\deg r \leq \deg b$ must be incorrect.

For uniqueness, consider two quotients q_1, q_2 and two remainders r_1, r_2 such that

$$a = bq_1 + r_1 = bq_2 + r_2.$$

Suppose for contradiction that $q_1 \neq q_2$. Then $\deg(q_2 - q_1) \geq 0$ and so

$$\deg(r_1 - r_2) = \deg(b(q_2 - q_1)) = \deg b + \deg(q_2 - q_1) \geq \deg b.$$

However, since $\deg r_1 < \deg b$ and $\deg r_2 < \deg b$, we have that $\deg(r_1 - r_2) \leq \max(\deg r_1, \deg r_2) < \deg b$. This is a contradiction, so we cannot have that $q_1 \neq q_2$.

Therefore we have that $q_1 = q_2$. Then

$$r_1 - r_2 = (a - bq_1) - (a - bq_2) = b(q_2 - q_1) = 0,$$

so $r_1 = r_2$.

(d) We mimic the proof by well-ordering of Bezout's identity for the integers. Consider the set

$$S = \{\deg(ay + bz) : y, z \text{ are polynomials}\}.$$

We claim that $S \neq \varnothing$ since $a \cdot 1 + b \cdot 0 = a$, so $\deg a \in S$.

Consider the polynomial d such that $\deg d \in S$ is the smallest element of S. Since $d \in S$, we have that $d = ay + bz$ for some polynomials y and z.

We show that $d = \gcd(a, b)$. We first show that $d \mid a$ and $d \mid b$. By the division algorithm, let q and r be the unique polynomials such that $a = dq + r$ and $\deg r < \deg d$. Then, if $r \neq 0$, we have that

$$\begin{aligned} r &= a - dq \\ &= a - (ay + bz)q \\ &= a(1 - y) + b(-zq). \end{aligned}$$

Therefore $\deg r \in S$. But $\deg r < \deg d$, so this is a contradiction to the fact that $\deg d$ is the least element of S. So our assumption that $r \neq 0$ is incorrect, and we have that $a = dq$. That is, $d \mid a$.

An identical argument shows that $d \mid b$.

Now consider any other common divisor c such that $c \mid a$ and $c \mid b$. Then $a = ck$ and $b = cj$ for some polynomials k and j, and so

$$\begin{aligned} d &= ay + bz \\ &= cky + cjz \\ &= c(ky + jz). \end{aligned}$$

So $\deg d = \deg c + \deg(ky + jz) \geq \deg c$.

So we have shown that for any other common divisor c, $\deg d \geq \deg c$. So d is the highest degree polynomial which is a common divisor of a and b. That is, $d = \gcd(a, b)$. Therefore we have found y and z such that

$$ay + bz = \gcd(a, b),$$

as desired.

2 The Polynomial Arithmetic

(a) We show (1) $\iff$ (3) as follows.

$$\begin{aligned} a \equiv b \pmod{m} &\iff m \mid (a - b) \\ &\iff \text{there exists a polynomial } k \text{ such that } a - b = km \\ &\iff \text{there exists a polynomial } k \text{ such that } a = km + b. \end{aligned}$$

We also show that (1) $\iff$ (2). By the division algorithm, let

$$\begin{aligned} a &= qm + r \\ b &= sm + t, \end{aligned}$$

where $r = a \bmod m$ and $t = b \bmod m$.

(2) $\implies$ (1). Suppose that $a \bmod m = b \bmod m$. Then $r = t$ and so

$$a - b = (qm + r) - (sm + t) = m(q - s) + (r - t) = m(q - s).$$

By definition, $m \mid (a - b)$, so $a \equiv b \pmod{m}$.

(1) $\implies$ (2). Suppose that $a \equiv b \pmod{m}$. Then $m \mid (a - b)$, where $(a - b) = m(q - s) + (r - t)$. So there is some polynomial k such that

$$m(q - s) + (r - t) = mk.$$

Therefore

$$r - t = m(k - q + s).$$

Suppose for contradiction that $k - q + s \neq 0$. Then $\deg(r - t) = \deg m + \deg(k - q + s) \geq \deg m$. But by the division algorithm, $\deg r < \deg m$ and $\deg t < \deg m$, so $\deg(r - t) \leq \max(\deg r, \deg t) < \deg m$. This is a contradiction, so it must be that $k - q + s = 0$. Therefore $r = t$, as desired.

Therefore (3) $\iff$ (1) $\iff$ (2). So the three are equivalent.

(b) We have that

$$\begin{aligned}
a \equiv b \pmod m &\iff m \mid (a-b) \\
&\iff \text{there exists some polynomial } k \text{ such that } a-b = mk \\
&\iff \text{there exists some polynomial } k \text{ such that } a(x)-b(x) = m(x)k(x) && \text{for all } x \in \mathbb{F}_p \\
&\iff m(x) \mid (a(x)-b(x)) && \text{for all } x \in \mathbb{F}_p \\
&\iff a(x) \equiv b(x) \pmod{m(x)} && \text{for all } x \in \mathbb{F}_p.
\end{aligned}$$

(c) By **(b)**, we have polynomials k and j such that $a = km + b$ and $c = jm + d$.

Then $a + c = km + b + jm + d = (k + j)m + b + d$. So again by **(b)**, $a + c \equiv b + d \pmod m$.

Similarly, $ac = (km + b)(jm + d) = (kjm + kd + jb)m + bd$. Again by **(b)**, $ac \equiv bd \pmod m$.

(d) Suppose $\gcd(a, m) = 1$. Then by Question 1**(d)**, there exist polynomials y and z such that

$$ay + mz = 1.$$

Therefore

$$ay = (-z)m + 1,$$

so by **(b)**, we have $ay \equiv 1 \pmod m$. So y is an inverse of a modulo m.

To show that it is unique, suppose there is another polynomial $v \neq y$ such that $av \equiv 1 \pmod m$. Then

$$\begin{aligned}
ay &\equiv 1 \pmod m \\
vay &\equiv v \pmod m \\
y &\equiv v \pmod m,
\end{aligned}$$

so they must be congruent modulo m.

(e) To solve this, we must find $(x^3)^{-1} \bmod x^2 + 1$. We do this using the extended Euclidean algorithm.

$$\begin{aligned}
\gcd(\boldsymbol{x^3}, \boldsymbol{x^2+1}) &= \gcd(\boldsymbol{x^2+1}, \boldsymbol{-x}) \\
&= \gcd(\boldsymbol{-x}, 1) \\
&= \gcd(1, 0) \\
&= 0.
\end{aligned}$$

$$\begin{aligned}
\boldsymbol{x^3} &= x \times (\boldsymbol{x^2+1}) + (\boldsymbol{-x}) \\
\boldsymbol{x^2+1} &= -x \times (\boldsymbol{-x}) + \boldsymbol{1} \\
\boldsymbol{-x} &= -x \times \boldsymbol{1} + \boldsymbol{0}
\end{aligned}$$

$$\begin{aligned}
\boldsymbol{-x} &= \boldsymbol{x^3} - x \times (\boldsymbol{x^2+1}) \\
\boldsymbol{1} &= \boldsymbol{x^2+1} + x \times (\boldsymbol{-x})
\end{aligned}$$

Iterating through the equations yields

$$\begin{aligned}
\boldsymbol{1} &= \boldsymbol{x^2+1} + x \times (\boldsymbol{-x}) \\
&= \boldsymbol{x^2+1} + x \times (\boldsymbol{x^3} - x \times (\boldsymbol{x^2+1})) \\
&= (1 - x^2)(\boldsymbol{x^2+1}) + x(\boldsymbol{x^3}).
\end{aligned}$$

Therefore $(x^3)^{-1} \equiv x \pmod{x^2+1}$. Thus we can solve the polynomial congruence.

$$\begin{aligned}
p(x)x^3 &\equiv x+1 && \pmod{x^2+1} \\
p(x)x^3x &\equiv (x+1)x && \pmod{x^2+1} \\
p(x) &\equiv x^2+x && \pmod{x^2+1} \\
p(x) &\equiv x-1 && \pmod{x^2+1},
\end{aligned}$$

where we get the last line from the fact that $x^2 + x = (x^2 + 1) + (x - 1)$.

Therefore any polynomial solution to the congruence is of the form $p(x) = k(x)(x^2 + 1) + (x - 1)$ for all x, for any polynomial k.

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) Given a specific set of k fixed points $x_1, \ldots, x_k$, we must map each of $f(x_1), \ldots, f(x_k)$ to $x_1, \ldots, x_k$, respectively.

We construct a permutation by choosing values for $f(1), f(2), \ldots, f(n)$ without replacement from $\{1, \ldots, n\}$. By the first rule of counting, there are $(n-k)!$ ways to do this, since the number of available values decreases by one for each choice made (as we cannot have $f(i) = f(j)$ for any $i \neq j$), and since each of the k fixed points have only one possible option ($f(x_i) = x_i$).

However, there are $\binom{n}{k}$ ways to choose which k values of $\{1, \ldots, n\}$ the fixed points will be, so the total number of permutations with at least k fixed points is

$$\binom{n}{k}(n-k)! = \frac{n!}{k!}.$$

(b) There are two ways to do this. One way is to partition on the value of x_1.

(1) If $x_1 = -3$, then we need $x_2 + x_3 + x_4 = n + 3$. Apply balls and bins. Since $x_4 \geq 3$, place 3 balls into x_4 and count the number of ways to distribute the remaining n balls among x_2, x_3, x_4. This is

$$\binom{n + (3-1)}{3-1} = \binom{n+2}{2}.$$

(2) If $x_1 = -2$, then we need $x_2 + x_3 + x_4 = n + 2$. Under the constraint that $x_4 \geq 3$, this is like throwing $n-1$ balls into three bins labelled x_2, x_3, and x_4. There are

$$\binom{n - 1 + (3-1)}{3-1} = \binom{n+1}{2}$$

ways to do this.

(3) If $x_1 = -1$, then we need $x_2 + x_3 + x_4 = n + 1$. Under the constraint that $x_4 \geq 3$, this is like throwing $n-2$ balls into three bins labelled x_2, x_3, and x_4. There are

$$\binom{n - 2 + (3-1)}{3-1} = \binom{n}{2}$$

ways to do this.

(4) If $x_1 \geq 0$, then we need $x_1 + x_2 + x_3 + x_4 = n$. Since $x_4 \geq 3$, throw 3 balls into the bin labelled x_4. Then count the ways to distribution $n-3$ balls among the four bins labelled x_1, x_2, x_3, and x_4. There are

$$\binom{n - 3 + (4-1)}{4-1} = \binom{n}{3}$$

ways to do this.

Each partition on x_1 is mutually exclusive, and together the partitions include all possible solutions. Therefore the number of integer solutions under the requested constraints is

$$\binom{n+2}{2} + \binom{n+1}{2} + \binom{n}{2} + \binom{n}{3}.$$

A more insightful approach is to transform the problem into a more standard balls-and-bins counting problem. Let $y_1 = x_1 + 3$ and $y_4 = x_4 - 3$. Then $y_1 \geq 0$, $y_4 \geq 0$, and

$$x_1 + x_2 + x_3 + x_4 = (y_1 - 3) + x_2 + x_3 + (y_4 + 3) = y_1 + x_2 + x_3 + y_4.$$

So any nonnegative integer solution to $y_1 + x_2 + x_3 + y_4 = n$ corresponds to an integer solution to $x_1 + x_2 + x_3 + x_4 = n$ subject to our constraints that $x_1 \geq -3$ $x_2, x_3 \geq 0$, and $x_4 \geq 3$.

The number of nonnegative integer solutions to $y_1 + x_2 + x_3 + y_4 = n$ is the number of ways to distribute n balls into 3 bins. That's

$$\binom{n + (4-1)}{4-1} = \binom{n+3}{3}.$$

(c) Let Q be the set of bridge hands with at least one quad. Then

$$Q = Q_1 \cup \ldots \cup Q_{13},$$

where Q_i is the set of bridge hands with a quad in rank i.

This will require inclusion-exclusion. However, note that $|Q_i \cap Q_j \cap Q_k \cap Q_\ell| = 0$, since there cannot be 4 quads in a hand of 13 cards. In fact, any intersection of the $Q_1, \ldots, Q_{13}$ involving more than 3 of the sets is empty.

Therefore, by the principle of inclusion-exclusion,

$$\begin{aligned}
|Q| &= \left|\bigcup_{i=1}^{13} Q_i\right| \\
&= \sum_{\{i\}} |Q_i| - \sum_{\{i,j\}} |Q_i \cap Q_j| + \sum_{\{i,j,k\}} |Q_i \cap Q_j \cap Q_k| \\
&= \binom{13}{1}|Q_1| - \binom{13}{2}|Q_1 \cap Q_2| + \binom{13}{3}|Q_1 \cap Q_2 \cap Q_3|,
\end{aligned}$$

where we use the symmetry in the ranks to see that the sizes of the intersections are all the same regardless of which ranks are participating in them.

To include a specific quad of a rank, we must select all cards from that rank. By the first rule of counting, we have that

$$\begin{aligned}
|Q_1| &= \binom{4}{4}\binom{48}{9}, \\
|Q_1 \cap Q_2| &= \binom{4}{4}\binom{4}{4}\binom{44}{5}, \\
|Q_1 \cap Q_2 \cap Q_3| &= \binom{4}{4}\binom{4}{4}\binom{4}{4}\binom{40}{1}.
\end{aligned}$$

Therefore

$$|Q| = \binom{13}{1}\binom{4}{4}\binom{48}{9} - \binom{13}{2}\binom{4}{4}\binom{4}{4}\binom{44}{5} + \binom{13}{3}\binom{4}{4}\binom{4}{4}\binom{4}{4}\binom{40}{1}.$$

(d) Let S be the set of sequences which include every element at least once. There is no easy way to find $|S|$ using the rules of counting. It may be tempting to place one ball into each of the bins and then count the number of ways to distribute the remaining $k - n$ balls, but this does not work; in particular, it overcounts since once another ball has been thrown into that bin, it is no longer necessary to have placed a ball in that bin beforehand.

Instead, we try finding the complement. There are n^k total sequences, and every sequence is either in S or in $S^{\mathrm{C}} = N$. Here, N is the set of sequences in which do not include at least one element. We can write

$$N = \bigcup_{i=1}^{n} N_i,$$

where N_i is the set of sequences which do not include element i. Then by the principle of inclusion-exclusion,

$$\begin{aligned}
|N| &= \left|\bigcup_{i=1}^{n} N_i\right| \\
&= \sum_{\{i\}} |N_i| - \sum_{\{i,j\}} |N_i \cap N_j| + \sum_{\{i,j,\ell\}} |N_i \cap N_j \cap N_\ell| - \ldots + (-1)^{n-1}\left|\bigcap_{i=1}^{n} N_i\right| \\
&= \binom{n}{1}|N_1| - \binom{n}{2}|N_1 \cap N_2| + \binom{n}{3}|N_1 \cap N_2 \cap N_3| - \ldots + (-1)^{n-1}\binom{n}{n}\left|\bigcap_{i=1}^{n} N_i\right|,
\end{aligned}$$

where we use the symmetry in the elements to see that the sizes of the intersections are all the same regardless of which sets are participating in them. For example, $|N_1 \cap N_2| = |N_3 \cap N_7| = |N_n \cap N_{n-1}|$.

By the first rule of counting, we have that

$$\begin{aligned}
|N_1| &= (n-1)^k, \\
|N_1 \cap N_2| &= (n-2)^k, \\
&\vdots \\
|N_1 \cap N_2 \cap \ldots \cap N_{n-1}| &= (n-(n-1))^k, \\
\left|\bigcap_{i=1}^{n} N_i\right| &= (n-n)^k.
\end{aligned}$$

Therefore

$$\begin{aligned}
|N| &= \binom{n}{1}|N_1| - \binom{n}{2}|N_1 \cap N_2| + \binom{n}{3}|N_1 \cap N_2 \cap N_3| - \ldots + (-1)^{n-1}\binom{n}{n}\left|\bigcap_{i=1}^{n} N_i\right| \\
&= \binom{n}{1}(n-1)^k - \binom{n}{2}(n-2)^k + \binom{n}{3}(n-3)^k - \ldots + (-1)^{n-1}\binom{n}{n}(n-n)^k.
\end{aligned}$$

Finally,

$$\begin{aligned}
|S| &= n^k - |N| \\
&= \binom{n}{0}(n-0)^k - \left(\binom{n}{1}(n-1)^k - \binom{n}{2}(n-2)^k + \binom{n}{3}(n-3)^k - \ldots + (-1)^{n-1}\binom{n}{n}(n-n)^k\right) \\
&= \sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^k.
\end{aligned}$$

(e) If an ace never appears in the first k cards, the first k cards must all be non-ace cards. There are 48 options for the first card, 47 options for the second card, and so on, until there are $48-(k-1)$ options for the k^{th} card.

The remaining cards can be any of the $52-k$ cards left. That is, there are $52-k$ options for the $(k+1)^{\text{th}}$ card, $52-k-1$ options for the $(k+2)^{\text{th}}$ card, and so on, until there is only one option for the 52^{nd} card.

By the first rule of counting, there are

$$48 \cdot 47 \cdot \ldots \cdot (48-(k-1)) \cdot (52-k) \cdot (52-k-1) \cdot \ldots \cdot 2 \cdot 1 = \frac{48!}{(48-k)!}(52-k)!$$

ways to do this.

4 The Catalan Numbers

(a) Antony always takes exactly n steps right and n steps up, for a total of $2n$ steps. The order in which Anthony takes these steps cannot change the number of steps he must take in each direction.

(b) Antony takes exactly $2n$ steps, where exactly n of these are steps to the right and the remaining n are steps up. There are $\binom{2n}{n}$ paths Anthony could take. Each path represents one way to choose n out of the $2n$ steps to be steps to the right.

(c) We can break the reflection of a point (x_0, y_0) across the line $y = x+1$ into two pieces: first, we shift the point to (x_0+1, y_0-1) and then we reflect it across the line $y = x$. Reflection across $y = x$ swaps the x- and y-coordinates. This means the point (x_0, y_0) gets transformed to (y_0-1, x_0+1) by reflection across the line $y = x+1$.

Applying this to an entire sequence of points yields the following function.

$$f((x_0,y_0),(x_1,y_1),\ldots,(x_{2n},y_{2n})) = ((y_0-1,x_0+1),(y_1-1,x_1+1),\ldots,(y_{2n}-1,x_{2n}+1)).$$

(d) The point where the path hits the fire will be reflected onto itself, so applying the reflection process will still result in a single unbroken path.

Any fiery path ends at point (n, n), and any such path reaches the endpoint after hitting the line $y = x+1$. Therefore, the endpoint (n, n) will be reflected. Applying the reflection process to (n, n) yields our new endpoint: $f((n,n)) = (n-1, n+1)$.

(e) Consider any two distinct fiery paths P and P', and let R and R' be the paths created by applying the reflection process to them, respectively. Since P and P' are distinct, there must differ along some edge. If that edge is before the reflection, then R and R' differ along that same edge; if that edge is after the reflection, then R and R' differ along the reflected edges.

(f) Any path R from $(0,0)$ to $(n-1,n+1)$ must cross the line $y=x+1$ at some point, since the starting point and ending point of such a path lie on opposite sides of the line. Applying the reflection process to such a path R yields a path P which ends at (n,n). Moreover, we know that P passes through the fire since R hits the line $y=x+1$, which is in the fire, and R and P are the same up until R hits the line $y=x+1$. So P passes through the fire and ends at (n,n), which means P is a fiery path.

(g) The reflection process gives a bijection between the set of fiery paths and the set of paths from $(0,0)$ to $(n-1,n+1)$. Part **(d)** shows that the reflection process is a well-defined function, **(e)** shows that the reflection process is an injection, and **(f)** shows that the reflection process is a surjection.

By the same reasoning as part **(b)**, Antony must take a total of $2n$ steps to walk from $(0,0)$ to $(n-1,n+1)$, and he must walk to the right exactly $n-1$ times, so there are $\binom{2n}{n-1}$ paths from $(0,0)$ to $(n-1,n+1)$. Therefore there must also be $\binom{2n}{n-1}$ fiery paths.

(h) There are $\binom{2n}{n}$ total paths, $\binom{2n}{n-1}$ of which pass through the fire. Therefore, there are

$$\binom{2n}{n}-\binom{2n}{n-1}$$

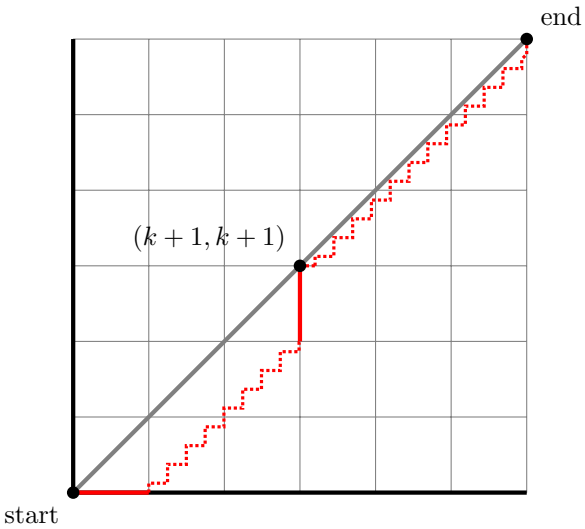
paths which do not touch the fire.

(i) By definition, the left-hand side of the identity counts the number of paths from $(0,0)$ to $(n+1,n+1)$ which do not touch the fire. We will call such paths *Catalan paths*.

By examining the right-hand side, we can see that it appears to be summing up, over k, the products of two Catalan paths, one of length k and one of length C_{n-k}. This motivates the following interpretation.

Observe that every Catalan path to $(n+1,n+1)$ must hit the diagonal for the first time at one of the diagonal points $(1,1),\ldots,(n+1,n+1)$. So we can count the total number of Catalan paths by counting the number of Catalan paths which hit the diagonal for the first time at $(1,1)$, the number which hit the diagonal for the first time at $(2,2)$, and so on, up to $(n+1,n+1)$.

Fix $k\in\{0,\ldots,n\}$ and consider all Catalan paths which hit the diagonal for the first time at $(k+1,k+1)$. Any such Catalan path will look like the following.



Observe that the dashed, zigzagged portions must be Catalan paths. There are C_k Catalan paths from $(0,1)$ to $(k+1,k)$, and there are C_{n-k} Catalan paths from $(k+1,k+1)$ to $(n+1,n+1)$. Therefore there are exactly C_kC_{n-k} Catalan paths which hit the diagonal for the first time at $(k+1,k+1)$. Summing this over each $k\in\{0,\ldots,n\}$ gets us every possible Catalan path from $(0,0)$ to $(n+1,n+1)$:

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

5 Earthquakes

(a) $N = N_1 \cap N_2 \cap N_3$. Therefore $N \subseteq N_1$, and hence $\mathrm{P}(N) \leq \mathrm{P}(N_1)$.

(b) By drawing a Venn diagram, we can see that

$$0.99 \leq \mathrm{P}(N_1 \cup N_2 \cup N_3) \leq 1.$$

That is, the chance is minimized when N_1 and N_2 are entirely contained within N_3, and it is certainly possible for the chance to be 1 in cases where the events do not totally overlap.

(c) We have already seen in **(a)** that $\mathrm{P}(N) \leq \mathrm{P}(N_1) = 0.93$. That is an upper bound, and it's the tightest upper bound we can get.

For the lower bound, consider the complement event

$$N^{\mathrm{C}} = N_1^{\mathrm{C}} \cup N_2^{\mathrm{C}} \cup N_3^{\mathrm{C}},$$

where $\mathrm{P}(N_1^{\mathrm{C}}) = 1 - \mathrm{P}(N_1) = 0.07$, $\mathrm{P}(N_2^{\mathrm{C}}) = 1 - \mathrm{P}(N_2) = 0.05$, and $\mathrm{P}(N_3^{\mathrm{C}}) = 1 - \mathrm{P}(N_3) = 0.01$.

By drawing these events in a Venn diagram, we can see that this chance is maximized when they are all mutually exclusive, and so

$$\mathrm{P}(N^{\mathrm{C}}) \leq \mathrm{P}(N_1^{\mathrm{C}}) + \mathrm{P}(N_2^{\mathrm{C}}) + \mathrm{P}(N_3^{\mathrm{C}}) = 0.07 + 0.05 + 0.01 = 0.13.$$

Therefore $\mathrm{P}(N) = 1 - \mathrm{P}(N^{\mathrm{C}}) \geq 1 - 0.13 = 0.87$.

So we have $0.87 \leq \mathrm{P}(N) \leq 0.93$.

(d) By drawing a Venn diagram, this is

$$\mathrm{P}(N_2) - \mathrm{P}(N_1 \cap N_2) = \mathrm{P}(N_2) - \mathrm{P}(N_2 \mid N_1)\mathrm{P}(N_1) = 0.95 - 0.99 \cdot 0.93.$$

6 Balls in Bins

(a) This is like throwing 11 balls into 26 bins labelled "A" through "Z". For the letters to spell probability, we must get 1 ball in each of the bins labelled "P," "R," "O," "A," "L," "T," and "Y," and 2 balls in each of the bins labelled "B" and "I."

The chance of any such sequence is $\left(\frac{1}{26}\right)^{11}$.

We must now count how many such sequences there are. There are 11! total ways to rearrange the 11 throws; however, the orders of the 2! ways to throw two balls into the "B" bin and the 2! ways to throw two balls in the "I" bin do not matter, so by the second rule of counting, there are 11!/2!2! such sequences.

So the probability is, by the addition rule

$$\frac{11!}{2!2!}\left(\frac{1}{26}\right)^{11}.$$

(b) This is like throwing 6 balls into 6 bins labelled with each of the 6 problems. For every student to ask about a different problem, we must get 1 ball in each of the six bins.

The chance of any such sequence of throws is $\left(\frac{1}{6}\right)^{6}$.

We must now count how many such sequences there are. The first ball has 6 possible bins, the second ball had 5 possible bins, and so on. By the first rule of counting, there are 6! sequences.

So the probability is, by the addition rule,

$$6!\left(\frac{1}{6}\right)^{6}.$$

(c) This is like throwing n balls into 6 bins labelled 1 through 6. For the face with six spots to never be rolled, we must have that no balls land in the sixth bin.

Let N_i be the event that the i^{th} ball does not land in the sixth bin. Then the event that there are no balls in the sixth bin is the same as the event that the first ball does not land in the sixth bin and the second ball does not land in the sixth bin, and so on.

$$\begin{aligned}
\mathrm{P}(\text{no balls in first bin}) &= \mathrm{P}(N_1 \cap N_2 \cap \ldots \cap N_n) \\
&= \mathrm{P}(N_1)\mathrm{P}(N_2) \cdot \ldots \cdot \mathrm{P}(N_n) && \text{(the throws are independent)} \\
&= \left(1 - \frac{1}{6}\right) \cdot \left(1 - \frac{1}{6}\right) \cdot \ldots \cdot \left(1 - \frac{1}{6}\right) && \text{(equally likely outcomes)} \\
&= \left(1 - \frac{1}{6}\right)^n.
\end{aligned}$$

(d) This is like throwing n balls into 6 bins labelled 1 through 6. For every face to be seen, there must be at least one ball in each bin.

It is very tempting to try and use stars and bars counting here: there are $\binom{n+5}{5}$ total ways to distribute the n balls into the 6 bins, and there are $\binom{n-1}{5}$ ways to distribute the n balls into the 6 bins such that every bin has at least one ball. However, we are erroneously assuming that every configuration of balls and bins is equally likely. This is not the case: there are many more ways to get, for example, about $n/6$ balls in each bin then there is for all n balls to land in the first bin. (There is only one way to get every ball in the first bin, however, there are many ways to throw the balls such that the balls are roughly evenly distributed among the bins.)

So our outcome space is the actual sequence of throws taken rather than the resulting configuration of balls into bins. Let A_i be the chance that the face with i spots is seen. Then the chance that every face is seen is

$$\mathrm{P}(A_1 \cap \ldots \cap A_6) = \mathrm{P}(A_1) \cdot \mathrm{P}(A_2 \mid A_1) \cdot \ldots \cdot \mathrm{P}(A_6 \mid A_1, \ldots, A_5).$$

Attempting to solve the probability this way will quickly get quite sticky when we get to the term $\mathrm{P}(A_2 \mid A_1)$. This would require partitioning over every possible number of times the face with one spot was seen. Things get even worse with $\mathrm{P}(A_3 \mid A_1, A_2)$.

So we start over with the complement. Let $N_i = A_i^{\mathrm{C}}$ be the event that the face with i spots is never seen. These events are easier to work with since there are much fewer ways to a face to be never seen than there are ways for a face to be seen. By De Morgan's laws for negating quantifiers, the complement of "all faces are seen" is "at least one face is not seen", so we have that

$$\mathrm{P}(A_1 \cap \ldots \cap A_6) = 1 - \mathrm{P}(N_1 \cup \ldots \cup N_6).$$

We cannot compute $\mathrm{P}(N_1 \cup \ldots \cup N_6)$ by the addition rule since the events are not mutually exclusive—it's possible that N_1 and N_2 both happen, for example if all n rolls show the face with six spots.

Therefore we must apply inclusion-exclusion. We have that

$$\mathrm{P}\left(\bigcup_{i=1}^{6} N_i\right) = \sum_{\{i\}} \mathrm{P}(N_i) - \sum_{\{i,j\}} \mathrm{P}(N_i \cap N_j) + \ldots - \mathrm{P}\left(\bigcap_{i=1}^{6} N_i\right).$$

Notice that by symmetry we have that $\mathrm{P}(N_1) = \mathrm{P}(N_2) = \ldots = \mathrm{P}(N_6)$, and that $\mathrm{P}(N_1 \cap N_2) = \mathrm{P}(N_2 \cap N_3) = \ldots = \mathrm{P}(N_5 \cap N_6)$ and so on. So the summands for each summation are identical to the other summands for that sum. So we can replace each sum of terms with simply the chance of any one term times the number of terms in that sum:

$$\begin{aligned}
\mathrm{P}\left(\bigcup_{i=1}^{6} N_i\right) &= \sum_{\{i\}} \mathrm{P}(N_i) - \sum_{\{i,j\}} \mathrm{P}(N_i \cap N_j) + \ldots - \mathrm{P}\left(\bigcap_{i=1}^{6} N_i\right) \\
&= \binom{6}{1}\mathrm{P}(N_1) - \binom{6}{2}\mathrm{P}(N_1 \cap N_2) + \ldots - \binom{6}{6}\mathrm{P}\left(\bigcap_{i=1}^{6} N_i\right).
\end{aligned}$$

Then we have, by extending the reasoning in part **(d)**, the following:

$$\begin{aligned}
\mathrm{P}(N_1) &= \left(1 - \frac{1}{6}\right)^n, \\
\mathrm{P}(N_1 \cap N_2) &= \left(1 - \frac{2}{6}\right)^n,
\end{aligned}$$

$$\vdots$$

$$\mathrm{P}\left(\bigcap_{i=1}^{6} N_i\right) = \left(1 - \frac{6}{6}\right)^n.$$

Therefore we have that

$$\mathrm{P}\left(\bigcap_{i=1}^{6} N_i\right) = \binom{6}{1}\mathrm{P}(N_1) - \binom{6}{2}\mathrm{P}(N_1 \cap N_2) + \ldots - \binom{6}{6}\mathrm{P}\left(\bigcap_{i=1}^{6} N_i\right) = \sum_{i=1}^{6}(-1)^{i-1}\binom{6}{i}\left(1 - \frac{i}{6}\right)^n.$$

So our final answer is

$$\begin{aligned}
\mathrm{P}\left(\bigcap_{i=1}^{n} A_i\right) &= 1 - \mathrm{P}\left(\bigcup_{i=1}^{n} N_i\right) \\
&= 1 - \sum_{i=1}^{6}(-1)^{i-1}\binom{6}{i}\left(1 - \frac{i}{6}\right)^n \\
&= \sum_{i=0}^{6}(-1)^{i}\binom{6}{i}\left(1 - \frac{i}{6}\right)^n.
\end{aligned}$$

Notice how this question is identical to Question 3**(d)**, except we have normalized by a denominator of 6^n.