Section C.1 – Counting

C.1-1 How many k-substrings does an n-string have? (Consider identical k-substrings at different positions to be different.) How many substrings does an n-string have in total?

For every position i of the n-string, $i = 1, \ldots, n-k+1$, there is one k-substring the starts at i and ends at $i+k-1$. Thus, the number of k-substrings in a n-string is

$$\sum_{i=1}^{n-k+1} 1 = n - k + 1.$$

Thus, the number of substrings (of all sizes) in an n-string is

$$\begin{aligned}\sum_{k=1}^{n} n - k + 1 &= n^2 + n - \sum_{k=1}^{n} k \\ &= n^2 + n - \frac{n(n+1)}{2} \\ &= n(n+1) - \frac{n(n+1)}{2} \\ &= \frac{n(n+1)}{2}.\end{aligned}$$

C.1-2 An n-input, m-output ***boolean function*** is a function from $\{\texttt{TRUE}, \texttt{FALSE}\}^n$ to $\{\texttt{TRUE}, \texttt{FALSE}\}^m$. How many n-input, 1-output boolean functions are there? How many n-input, m-output boolean functions are there?

We can view the number of possible inputs of size n as the number of binary n-strings, which is 2^n.

Now, consider a single-valued function from $\{\texttt{TRUE}, \texttt{FALSE}\}^n$ to $\{\texttt{TRUE}\}$. In this case, the number of possible functions is the number of possible inputs, which is 2^n. Since an 1-output boolean function has two possible output values, each of the 2^n functions we referred in the case of a single-valued function now has two ways to pick the output value. We can view this number as the number of binary 2^n-strings, which is 2^{2^n}. As for an n-output function, each of the 2^n functions we referred in the case of a single-valued function now has 2^m ways to pick the output value. Thus, there are $(2^m)^{2^n}$ of those.

C.1-3 In how many ways can n professors sit around a circular conference table? Consider two seatings to be the same if one can be rotated to form the other.

For two seatings to be different from each other, the ordering of professors in each seating needs to be different. This number can be viewed as the number of permutations of a set n elements, which is $n!$. However, note that for each permutation that starts with professor k, $1 \leq k \leq n$, there are $n-1$ other permutations that are just a rotation of it. For instance, the seatings $\{2,3,1\}$ and $\{3,1,2\}$ are a rotation of $\{1,2,3\}$. Thus, the number of different seatings can be viewed as fixing the seat of the first professor and computing the number of permutations of the remaining $n-1$ professors, which is $(n-1)!$.

C.1-4 In how many ways can we choose three distinct numbers from the set $\{1, 2, \ldots, 99\}$ so that their sum is even?

The set has 50 odd numbers and 49 even numbers. For the sum be even, we have to choose three even numbers or one even and two odds. For the case with three even numbers, there are $49!/(3! \cdot (49-3)!) = 18424$ ways of choosing 3 distincts numbers among the 49 even numbers. As for the case with one even and two odds, there are 49 ways to choose one even number and $50!/(2! \cdot (50-2)!) = 1225$ ways of choosing 2 distincts numbers among the 50 odd numbers. Thus, there are $18424 + 49 \cdot 1225 = 78449$ ways to get an even sum.

C.1-5 Prove the identity

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$$

for $0 < k \leq n$.

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{k! \cdot (n-k)!} \\ &= \frac{n \cdot (n-1)!}{k \cdot (k-1)! \cdot (n-k)!} \\ &= \frac{n}{k}\frac{(n-1)!}{(k-1)! \cdot ((n-1)-(k-1))!} \\ &= \frac{n}{k}\binom{n-1}{k-1}.\end{aligned}$$

C.1-6 Prove the identity

$$\binom{n}{k} = \frac{n}{n-k}\binom{n-1}{k}$$

for $0 \leq k < n$.

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{k! \cdot (n-k)!} \\ &= \frac{n \cdot (n-1)!}{k! \cdot (n-k) \cdot (n-k-1)!} \\ &= \frac{n}{n-k}\frac{(n-1)!}{k! \cdot ((n-1)-k)!} \\ &= \frac{n}{n-k}\binom{n-1}{k}.\end{aligned}$$

C.1-7 To choose k objects from n, you can make one of the objects distinguished and consider whether the distinguished object is chosen. Use this approach to prove that

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Let $S = \{s_1, s_2, \ldots, s_{n-1}\}$ and s_0 the distinguished element. To choose k from the n elements, we have to consider two cases:

(a) If s_0 is selected, it will be necessary to choose the $k-1$ remaining elements from S. There are $\binom{n-1}{k-1}$ combinations.

(b) If s_0 is not selected, it will be necessary to choose the k remaining elements from S. There are $\binom{n-1}{k}$ combinations.

Adding the above together, we have

$$\begin{aligned}\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)! \cdot (n-k)!} + \frac{(n-1)!}{k! \cdot (n-k-1)!} \\ &= \frac{k \cdot (n-1)!}{k! \cdot (n-k)!} + \frac{(n-k) \cdot (n-1)!}{k! \cdot (n-k)!} \\ &= \frac{(k+n-k) \cdot (n-1)!}{k! \cdot (n-k)!} \\ &= \frac{n!}{k! \cdot (n-k)!} \\ &= \binom{n}{k}.\end{aligned}$$

C.1-8 Using the result of Exercise C.1-7, make a table for $n = 0, 1, \ldots, 6$ and $0 \le k \le n$ of the binomial coefficients $\binom{n}{k}$ with $\binom{0}{0}$ at the top, $\binom{1}{0}$ and $\binom{1}{1}$ on the next line, and so forth. Such a table of binomial coefficients is called ***Pascal's triangle***.

The table with binomials

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$

$$\binom{5}{0} \quad \binom{5}{1} \quad \binom{5}{2} \quad \binom{5}{3} \quad \binom{5}{4} \quad \binom{5}{5}$$

$$\binom{6}{0} \quad \binom{6}{1} \quad \binom{6}{2} \quad \binom{6}{3} \quad \binom{6}{4} \quad \binom{6}{5} \quad \binom{6}{6}$$

Using the above table and the result of C.1-7, we have the Pascal's triangle

$$1$$

$$1 \quad 1$$

$$1 \quad 2 \quad 1$$

$$1 \quad 3 \quad 3 \quad 1$$

$$1 \quad 4 \quad 6 \quad 4 \quad 1$$

$$1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1$$

$$1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1$$

C.1-9 Prove that

$$\sum_{i=1}^{n} i = \binom{n+1}{2}.$$

We have

$$\begin{aligned}
\binom{n+1}{2} &= \frac{(n+1)!}{2! \cdot ((n+1)-2)!} \\
&= \frac{(n+1) \cdot n \cdot (n-1)!}{2 \cdot (n-1)!} \\
&= \frac{n(n+1)}{2} \\
&= \sum_{i=1}^{n} i,
\end{aligned}$$

which also shows that the third Pascal's diagonal has the triangular numbers.

C.1-10 Show that for any integers $n \geq 0$ and $0 \leq k \leq n$, the expression $\binom{n}{k}$ achieves its maximum value when $k = \lfloor n/2 \rfloor$ or $k = \lceil n/2 \rceil$.

It follows from the Pascal's triangle

$$\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1 \\
\vdots
\end{array}$$

We can prove by induction. The base case, which occurs when $n = 0$, holds since

$$\binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} = \binom{0}{0} = 1$$

is maximum on row 0. Now, assume it holds for n. Then, if $n+1$ is even, from Equation (C.3) we have

$$\begin{aligned}
\binom{n+1}{\lfloor \frac{n+1}{2} \rfloor} = \binom{n+1}{\lceil \frac{n+1}{2} \rceil} &= \binom{n}{(\frac{n+1}{2} - 1)} + \binom{n}{(\frac{n+1}{2})} \\
&= \binom{n}{(\frac{n}{2} - \frac{1}{2})} + \binom{n}{(\frac{n}{2} + \frac{1}{2})} \qquad \text{(since } n \text{ is odd)} \\
&= \binom{n}{\lfloor \frac{n}{2} \rfloor} + \binom{n}{\lceil \frac{n}{2} \rceil},
\end{aligned}$$

which shows that is also holds for $n+1$ since

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} \text{ and } \binom{n}{\lceil \frac{n}{2} \rceil}$$

are both maximum on row n. The proof is similar when $n+1$ is odd.

C.1-11 ($\star$) Argue that for any integers $n \geq 0$, $j \geq 0$, $k \geq 0$, and $j + k \leq n$,

$$\binom{n}{j+k} \leq \binom{n}{j}\binom{n-j}{k}.$$

Provide both an algebraic proof and an argument based on a method for choosing $j+k$ items out of n. Give an example in which equality does not hold.

For any integers $a \geq 0, b \geq 0$, and $a \geq b$, we have

$$\begin{aligned}(a+b)! &= \underbrace{(a+b)\cdot(a+b-1)\cdot(a+b-2)\cdots}_{b \text{ times}} a!\\ &\geq \underbrace{b\cdot(b-1)\cdot(b-2)\cdots}_{b \text{ times}} a!\\ &= a!\cdot b!.\end{aligned}$$

Using the above result, we have

$$\begin{aligned}\binom{n}{j}\binom{n-j}{k} &= \frac{n!}{j!\cdot(n-j)!}\frac{(n-j)!}{k!\cdot((n-j)-k)!}\\ &= \frac{n!}{j!\cdot k!\cdot((n-j)-k)!}\\ &\geq \frac{n!}{(j+k)!\cdot(n-(j+k))!}\\ &= \binom{n}{j+k}.\end{aligned}$$

The expression on the left is the number of ways to choose an $(j+k)$-subset of an n-set (which leaves the reamining $n-(j+k)$ elements). Thus, it is a partition of the original n-set into subsets of cardinalities $(j+k)$ and $n-(j+k)$. The right hand side has two factors: the first binomial coefficient is the number of ways to choose a j-subset of an n-set (which leaves the reamining $n-j$ elements); the second is the number of ways to choose a k-subset from the remaining $n-j$ elements. Thus, it is a partition of the original n-set into subsets of cardinalities j, k, and $n-(j+k)$. Consider now that we choose the $n-(j+k)$ first, leaving behind the remaining $j+k$ elements. There is precisely one way to choose an $(j+k)$-subset out of the remaining $j+k$ elements. On the other hand, when we first choose j and then we choose k, if $j < j+k$, there are *at least* two ways to choose a j-subset from the $(j+k)$-subset and precisely one way to choose a k-subset from the remaining k elements. This notion also applies to the algebraic proof, since $(j+k)! = j!\cdot k \iff j = 0$ or $k = 0$. Also note that while the left expression does not count any permutation of the $(j+k)$-subsets (since it normalizes by $(j+k)!$), the right expression, despite not counting permutations of each of the subsets indepentently (since it normalizes by $j!\cdot k!$), it counts permutations of two subsets together. For instance, let $A = \{a, b\}$. There is only one way to choose 2 elements from A, which is ab. However, there are two ways to choose one element and then another element from A, which are ab and ba.

C.1-12 ($\star$) Use induction on all integers k such that $0 \leq k \leq n/2$ to prove inequality (C.6), and use equation (C.3) to extend it to all integers k such that $0 \leq k \leq n$.

Skipped.

C.1-13 ($\star$) Use Stirling's approximation to prove that

$$\binom{2n}{n} = \frac{2^{2n}}{\sqrt{\pi n}}(1 + O(1/n)).$$

Skipped.

C.1-14 ($\star$) By differentiating the entropy function $H(\lambda)$, show that it achieves its maximum value at $\lambda = 1/2$. What is $H(1/2)$?

Skipped.

C.1-15 ($\star$) Show that for any integer $n \geq 0$,

$$\sum_{k=0}^{n} \binom{n}{k} k = n2^{n-1}.$$

Skipped.

Section C.2 – Probability

C.2-1 Professor Rosencrantz flips a fair coin once. Professor Guildenstern flips a fair coin twice. What is the probability that Professor Rosencrantz obtains more heads than Professor Guildenstern?

The sample space $\{\mathrm{H},\mathrm{T}\}^3$ has size $2^3 = 8$. Since the only event that satisfies the condition is $\{\mathrm{HTT}\}$, the probability is $1/8$.

C.2-2 Prove the ***Boole's inequality***: For any finite or countably infinite sequence of events $A_1, A_2, \ldots,$

$$\Pr\{A_1 \cup A_2 \cup \cdots\} \le \Pr\{A_1\} + \Pr\{A_2\} + \cdots .$$

From (C.13) we have

$$\Pr\{A_1 \cup A_2\} \le \Pr\{A_1\} + \Pr\{A_2\},$$

which implies

$$\begin{aligned}\Pr\{A_1 \cup A_2 \cup \cdots\} &= \Pr\{A_1 \cup (A_2 \cup \cdots)\} \\ &\le \Pr\{A_1\} + \Pr\{A_2 \cup (A_3 \cup \cdots)\} \\ &\le \Pr\{A_1\} + \Pr\{A_2\} + \Pr\{A_3 \cup (A_4 \cup \cdots)\} \\ &\le \Pr\{A_1\} + \Pr\{A_2\} + \Pr\{A_3\} \cdots .\end{aligned}$$

C.2-3 Suppose we shuffle a deck of 10 cards, each bearing a distinct number from 1 to 10, to mix the cards thoroughly. We then remove three cards, one at a time, from the deck. What is the probability that we select the three cards in sorted (increasing) order?

Let $a < b < c$ denote the number of the three selected cards. There are 3! permutations of $\{a, b, c\}$ and abc is the only one which is in sorted order. Thus, the probability is $1/3! = 1/6$.

C.2-4 Prove that

$$\Pr\{A \mid B\} + \Pr\{\overline{A} \mid B\} = 1.$$

We have

$$\begin{aligned}\Pr\{B\} &= \Pr\{(B \cap A) \cup (B \cap \overline{A})\} \\ &= \Pr\{B \cap A\} + \Pr\{B \cap \overline{A}\} \\ &= \Pr\{A\}\Pr\{B \mid A\} + \Pr\{\overline{A}\}\Pr\{B \mid \overline{A}\}.\end{aligned}$$

Substituting into (C.17) yields

$$\begin{aligned}\Pr\{A \mid B\} + \Pr\{\overline{A} \mid B\} &= \frac{\Pr\{A\}\Pr\{B \mid A\}}{\Pr\{B\}} + \frac{\Pr\{\overline{A}\}\Pr\{B \mid \overline{A}\}}{\Pr\{B\}} \\ &= \frac{\Pr\{A\}\Pr\{B \mid A\} + \Pr\{\overline{A}\}\Pr\{B \mid \overline{A}\}}{\Pr\{B\}} \\ &= \frac{\Pr\{A\}\Pr\{B \mid A\} + \Pr\{\overline{A}\}\Pr\{B \mid \overline{A}\}}{\Pr\{A\}\Pr\{B \mid A\} + \Pr\{\overline{A}\}\Pr\{B \mid \overline{A}\}} \\ &= 1.\end{aligned}$$

C.2-5 Prove that for any collection of events $A_1, A_2, \ldots, A_n$,

$$\Pr\{A_1 \cap A_2 \cap \cdots \cap A_n\} = \Pr\{A_1\} \cdot \Pr\{A_2 \mid A_1\} \cdot \Pr\{A_3 \mid A_1 \cap A_2\} \cdots \Pr\{A_n \mid A_1 \cap A_2 \cap \cdots \cap A_{n-1}\}.$$

It is trivially valid for $n = 1$. As our base case, consider $n = 2$. From (C.16) we have

$$\Pr\{A_1 \cap A_2\} = \Pr\{A_1\}\Pr\{A_2 \mid A_1\}.$$

Now assume it holds for n. For $n+1$, we have

$$\begin{aligned}\Pr\{A_1 \cap A_2 \cap \cdots \cap A_{n+1}\} &= \Pr\{(A_1 \cap A_2 \cap \cdots \cap A_n) \cap A_{n+1}\} \\ &= \Pr\{A_1 \cap A_2 \cap \cdots \cap A_n\}\Pr\{A_{n+1} \mid A_1 \cap A_2 \cap \cdots \cap A_n\} \\ &= \Pr\{A_1\} \cdot \Pr\{A_2 \mid A_1\} \cdot \Pr\{A_3 \mid A_1 \cap A_2\} \cdots \Pr\{A_{n+1} \mid A_1 \cap A_2 \cap \cdots \cap A_n\}.\end{aligned}$$

C.2-6 ($\star$) Describe a procedure that takes as input two integers a and b such that $0 < a < b$ and, using fair coin flips, produces as output heads with probability a/b and tails with probability $(b-a)/b$. Give a bound on the expected number of coin flips, which should be $O(1)$. (Hint: Represent a/b in binary.)

Consider a continuous uniform probability distribution on $[0,1)$, such that $\Pr\{[0,1)\} = 1$. We have

$$\Pr\left\{\left[0, \frac{a}{b}\right)\right\} = \frac{a}{b},$$

and

$$\Pr\left\{\left[\frac{a}{b}, 1\right)\right\} = 1 - \frac{a}{b} = \frac{b-a}{b}.$$

With this notion, we can write a procedure that sorts a real number from $[0,1)$ and return heads if it is lower than a/b or return tails, otherwise. Using fair coin flips and representing numbers in binary, for each flip we have a new decimal place from a random number on $[0,1)$ (consider an “0” if the coin flip is head and “1”, otherwise). Then,

- if the i-th flip is 1 and the i-th decimal place of a/b is 0, the sorted number is larger than a/b and we return tails;
- if the i-th flip is 0 and the i-th decimal place of a/b is 1, the sorted number is smaller than a/b and we return head;
- if the i-th flip and the i-th decimal place are equal, we sort a new decimal place.

Since we do not know how many decimal places a/b has (if periodic, this number is infinite), the above procedure does not have a maximum number of iterations. However, since for each flip we have a probability of $1/2$ of returning head or tails, the probability of terminating at flip i, for $i \geq 1$, is

$$\underbrace{1/2 \cdot 1/2 \cdots}_{i \text{ times}} = \frac{1}{2^i}.$$

Thus, by using the notion of expected value and the result (A.8), the expected number of flips is

$$\sum_{i=1}^{\infty} i \cdot \frac{1}{2^i} = \sum_{i=0}^{\infty} i \cdot \left(\frac{1}{2}\right)^i = \frac{1/2}{(1-1/2)^2} = 2.$$

C.2-7 ($\star$) Show how to construct a set of n events that are paiwise independent but such that no subset of $k > 2$ of them is mutually independent.

Answer.

C.2-8 ($\star$) Two events A and B are ***conditionally independent***, given C, if

$$\Pr\{A \cap B \mid C\} = \Pr\{A \mid C\} \cdot \Pr\{B \mid C\}.$$

Give a simple but nontrivial example of two events that are not independent but are conditionally independent given a third event.

Answer.

C.2-9 ($\star$) You are a contestant in a game show in which a prize is hidden behind one of three curtains. You will win the prize if you select the correct curtain. After you have picked one curtain but before the curtain is lifted, the emcee lifts one of the other curtains, knowing that it will reveal an empty stage, and asks if you would like to switch from your current selection to the remaining curtain. How would your chances change if you switch? (This question is the celebrated ***Monty Hall problem***, named after a game-show host who often presented contestants with just this dilemma.)

If you never switch, the only way to win is to choose the right curtain at the beginning (before the emcee lifts one of the others). In this case, your chance to win are $1/3$. If you always switch, the only way to loose is to choose the right curtain at the beginning. In this case, when you choose a curtain without the prize, the emcee will reveal the other empty curtain and you will therefore change to the correct one. Thus, your chance to win are $(1 - 1/3) = 2/3$.

C.2-10 ($\star$) A prison warden has randomly picked one prisoner among three to go free. The other two will be executed. The guard knows which one will go free but is forbidden to give any prisoner information regarding his status. Let us call the prisoners X, Y, and Z. Prisoner X asks the guard privately which of Y or Z will be executed, arguing that since he already knows that at least one of them must die, the guard won't be revealing any information about his own status. The guard tells X that Y is to be executed. Prisoner X feels happier now, since he figures that either he or prisoner Z will go free, which means that his probability of going free is now $1/2$. Is he right, or are his chances still $1/3$? Explain.

His chances are still $1/3$. Let A be the event of prisoner X going free and B the event that the guard tells X that Y is to be executed. We have

$$\Pr(A \mid B) = \frac{\Pr(A)\Pr(B \mid A)}{\Pr(B)} = \frac{1/3 \cdot 1/2}{1/2} = \frac{1}{3}.$$