Toddler Probability

Jes Modian

February 9, 2023

Abstract

As a gaming addict, I can certainly say that probability comes up a lot when I am playing games. I will never forget the frustration of grinding for wither skeleton skulls and never getting one after killing more than 100 wither skeletons in Minecraft. How does that make any sense? Probability is a fascinating subject, and has many properties that does not follow our intuition. That's why I want to explain it in detail.

Contents

0 Introduction

0.1 Randomness

When something random happens, it involves probability. A random **experiment** or **trial** is an action with an outcome that we cannot determine with absolute certainty. It can be throwing a dice, flipping a coin, drawing a ball from a bag, drawing balls from a shuffled deck, etc. When we repeat the same experiment several times, each conduction of the experiment is called a trial. When many trials is conducted in an experiment, the sequence of outcomes will not have a certain pattern or cycle. There is also not a deterministic algorithm [1] that can generate the outcome. So the outcome of a random experiment is unpredictable. We can only predict the frequency of the different outcomes generated by the experiments.

Take flipping a fair coin for example. It has two possible outcomes, head (H) or tail (T). When we flip a coin many times, the sequence of outcome will not always be a pattern, such as always generating heads after tails (HTHTHTHTHTHTHTHTHTHTHT......). It will be more like HTHTH-HTHTHHTHHHTTHHTTTHHTTTHTHTTTHHTHHHTTTTHTHHHTH ...... Even when we flip the coin 50 times and observe the outcomes, we will not know whether the outcomes of the next coin flip is H or T. However, when we continue flipping the coin many many times and record the outcomes, we will find that H and T appear roughly the same amount of times (the relative difference between H and T is small).

0.2 Probability and event

This is where the concept of probability comes in. **Probability** (sometimes called chance) is the measure of how likely something will happen, with a numerical value between 0 and 1 (inclusive). This 'something' is called an **event**. Every event can be assigned a probability, and the more likely an event will happen, the higher the probability is. An event with a probability of 1 has an absolute certainty of happening, and an event with 0 probability will never happen (meaning the event is impossible to happen). Probability can be expressed as a fraction, a decimal number, or a percentage.

In the above example of flipping coins, the event 'getting a head' or the event 'getting a tail' are equally likely to happen. We also know that a coin flip either produces a head or a tail. It cannot produce both head and tail, or other stuff like a '6' in a dice throw. So the probability of the event "gettiing a head **or** getting a tail" has a probability of 1. So both the event 'getting a head' and the event 'getting a tail' have a $\frac{1}{2}$ (or 0.5 or 50%) probability of happening.

Besides coin flips, we can also define events in other experiments. A random event can be getting an '6' in a dice throw, drawing a white ball from a bag of balls with different colours, drawing $\heartsuit 8$ from a deck of poker balls, etc. It can even happen across multiple trials of an experiment, such

[1] A deterministic algorithm, when given a particular input, will always generate the same output. An example is the algorithm that produces the decimal expansion of $\sqrt{2}$.

as getting two heads in two coin flips, getting ‘6’ three times in a row, etc.

Mathematically, we can denote an event by a capital letter, such as A, B, C, etc. The probability of the event A is denoted by $P(A)$. The probability of an event happening in an experiment is a ratio. Hypothetically, if the experiment was to be repeated many many times, the ratio of the number of times the event will happen, to the total number of trials (how many times the experiment is repeated) will **converge** to the probability of the event. This means the value of the ratio will eventually get closer and closer to the probability, instead of bouncing around forever. This is the **law of large numbers**, and we can express it as:

$$P(A) \approx \frac{\text{Number of times } A \text{ will happen}}{\text{Number of trials}}$$

as the number of trials tends towards infinity (the experiment is repeated forever).

For example, if we flip a fair coin a trillion times, heads and tails will each appear roughly 0.5 trillion times (but rarely exactly 0.5 trillion times due to the fluctuating nature of probability). If we flip the coin 10^{100} times, the ratio $\frac{\text{number of heads}}{10^{100}}$ will get even closer to 0.5, which is the probability of a single head in a single coin flip.

0.3 Outcome and sample space

Conducting experiments can lead to different **outcomes**. A coin flip has the possible outcomes of head (H) and tails (T). A dice throw has the possible outcomes of ‘1’ , ‘2’ , ‘3’ , ‘4’ , ‘5’ , ‘6’ . The possible outcomes are **mutually exclusive**[2] (or **disjoint**) to one another, meaning a trial of the experiment can only lead to exactly one outcome at the same time. A coin flip cannot land on both H and T , and a dice throw cannot land on both ‘1’ and ‘2’. Different outcomes must happen across multiple trials.

The set of all possible outcomes of an experiment is called the **sample space**, typically denoted by Ω. The sample space of a coin flip is $\{\mathrm{H}, \mathrm{T}\}$, and the sample space of a dice throw is $\{1, 2, 3, 4, 5, 6\}$.

We can define an event to happen when the outcome of the experiment satisfy certain conditions. In a dice throw, the event can be getting a ‘6’ , or getting an even number. An event A can be expressed or treated as a **subset** of the sample space Ω (denoted by $A \subseteq \Omega$). The event set of getting a ‘6’ is

[2] When some events or outcomes are mutually exclusive/disjoint to one another, only one of them can happen at the same time. When one event happens, it implies that all the other event do not happen.

$\{6\}$, and the event set of getting an even number is $\{2, 4, 6\}$. The outcomes (elements) in an event set are called **desired outcomes**. If an experiment is conducted, and the outcome is in the event set, then the event happens. Otherwise the event does not happen. Note that the same event set can include different outcomes, and the same outcome can belong to different event sets.

Outcomes have a probability to occur, and each individual outcome also has a probability assigned to it, just like events. The difference between events and outcomes is that events are sets that contain some outcomes of an experiment, and outcomes are the elements of the event sets. The probability of all of the outcomes in the same experiment sums up to 1, because it is certain that one of the outcomes will occur in an experiment, and they are all disjoint. However, the probability of all of the events in an experiment may sum up to more or less than 1, since more than one events can happen in the same experiment, or there can be none of the events happening.

0.4 Axioms of probability

There are three **axioms of probability** [1], from which we can deduce other properties:

1. For any event A , $P(A) \geq 0$.
2. Probability of the sample space Ω is $P(\Omega) = 1$.
3. If $A_1, A_2, A_3, \ldots$ are disjoint events, then $P(A_1 \cup A_2 \cup A_3 \cup \ldots) = P(A_1) + P(A_2) + P(A_3) + \ldots$

Axiom 1 states that the probability of an event is non-negative. Axiom 2 ensures that the sum of probability of all outcomes in the sample space is 1. Axiom 3 says that we can add the individual probabilities of any number of disjoint events to get the probability of their union, even if the number of events is **countably infinite** [3]. (We will go into the details later... Probably never. I'm tired. My life is a joke.)

[3] When there are countably infinite number of something, we can label each of them with a distinct natural number, that is, we can map each of them to a natural number with one-to-one correspondence.

1 Simple probability problems

1.1 Uniform probability

Let us consider an experiment in which there are N possible outcomes, and every outcome has an equal (uniform) probability of occurring. Since the probability of getting an outcome that *belongs to* the sample space is 1, the probability of getting a particular outcome is $\frac{1}{N}$. This probability is the same for each of the possible outcomes.

Theorem 1.1. If there is an experiment with N possible outcomes that have uniform probability of occurring, and x is one of the outcomes, then

$$P(x) = \frac{1}{N}$$

Note that an event that has only one desired outcome has the same probability of that desired outcome. (If $A = \{x\}, \text{then} \quad P(A) = P(x)$.)

Let us practice with a problem.

Problem 1. When throwing a fair dice, what is the probability of getting a '6' ?

(Difficulty level: 1)

Solution 1. There are 6 possible outcomes when throwing a fair dice, and only 1 desired outcome. Putting $N = 6$, we get the answer $\boxed{\frac{1}{6}}$.

What if the event has more than one desired outcome? Let the other conditions of the above situation stay the same (there are N equally probable possible outcomes).

In that case, the probability of the event (denoted by A) is:

$$P(A) = \frac{\text{Number of desired outcomes}}{\text{Number of possible outcomes}}$$

Written in another way, we have:

$$P(A) = \frac{|A|}{N} \quad \text{or} \quad P(A) = \frac{|A|}{|\Omega|}$$

, where $|A|$ is the number of elements in the event set A, and $|\Omega|$ $(= N)$ is the number of elements in the sample space Ω.

Theorem 1.2. If there is an experiment with N possible outcomes that have uniform probability of occurring, and A is an event of the sample space, then

$$P(A) = \frac{|A|}{N}$$

Problem 2. When throwing a fair dice, what is the probability of getting a prime number?

(Difficulty level: 2)

Solution 2. The desired outcomes are prime numbers in the set $\{1, 2, 3, 4, 5, 6\}$, so the set of desired outcomes is $\{2, 3, 5\}$, which has 3 elements. The number of possible outcomes is still 6. So $P(\text{prime number}) = \frac{3}{6} = \boxed{\frac{1}{2}}$.

1.2 Compound events

Compound events consist of two or more events, joined by '**and**' or '**or**'. Let A, B be events. The event that both A and B happen is a compound event, denoted by $A \cap B$. The event that A or B or both A and B happens is also a compound event, denoted by $A \cup B$. ($\cap$ is called **intersection** and $\cup$ is called **union**. Recall that in set language, $A \cap B$ is the set of all elements that are in both A and B, and $A \cup B$ is the set of all elements that are in A or B or both. The two interpretation of sets and events are equivalent.) There can be more complicated compound events, such as $A \cup (B \cap C)$, or $A \cup B \cup C \cup D \cup E$, but now we only consider compound events that consist of two events.

1.2.1 Union of disjoint events

What if there are two disjoint events A, B in the same sample space (of a single experiment), and we need to find the probability that A happens **or** B happens? (Notice that when two events are disjoint, so are their event sets, meaning their event sets will not contain any common elements, and it is denoted by $A \cap B = \varnothing$.) In that case, the set of desired outcomes is the union of A and B (written as $A \cup B$), and what we are trying to find is $P(A \cup B)$. There are two equivalent ways to find the probability. We can count the total number of elements in $A \cup B$, then divide it by the total number of possible outcomes. The other way is to simply add the two events' individual probabilities together. We have the simple **addition rule**:

Theorem 1.3. If A, B are disjoint events, then

$$P(A \cup B) = P(A) + P(B)$$

To see why, notice that when sets A, B are disjoint, we have:

$$|A| + |B| = |A \cup B|$$

Also,

$$P(A \cup B) = \frac{|A \cup B|}{|\Omega|}$$

$$\text{Thus,} \qquad \begin{aligned} P(A) + P(B) &= \frac{|A|}{|\Omega|} + \frac{|B|}{|\Omega|} \\ &= \frac{|A| + |B|}{|\Omega|} \\ &= \frac{|A \cup B|}{|\Omega|} \\ &= P(A \cup B) \end{aligned}$$

The addition rule holds true for more than two disjoint events. In general, if there are n disjoint events labelled $A_1, A_2, \ldots, A_n$, then

$$P(A_1 \cup A_2 \cup \ldots \cup A_n) = P(A_1) + P(A_2) + \ldots + P(A_n)$$

Problem 3. A bag contains 5 red balls, 3 blue balls and 7 green balls. Randomly draw a ball from the bag. What is the probability that it is a blue ball or a green ball?

(Difficulty level: 2)

Solution 3a. Let A be the event 'drawing a blue ball', and B be the event 'drawing a green ball'. The set of desired outcomes ($A \cup B$) are all the blue balls and green balls. Since A and B are disjoint, we can add the blue balls and green balls together to get the number of desired outcomes, which is 3+7. The total number of possible outcomes is 3+5+7. So $P(A \cup B) = \frac{3+7}{3+5+7} = \frac{10}{15} = \boxed{\frac{2}{3}}$.

Solution 3b. The total number of possible outcomes is 3+5+7=15 . Notice that $P(A) = \frac{3}{15}$ and $P(B) = \frac{7}{15}$, so $P(A \cup B) = \frac{3}{15} + \frac{7}{15} = \boxed{\frac{2}{3}}$.

1.2.2 Intersection and union of two events

Now, what if there are two non-disjoint events A, B in the same sample space (of a single experiment), and we need to find the probability that both A and B happen? Let's consider an example:

Problem 4.1. Randomly draw an integer from 1 to 12 inclusive. What is the probability that it is a prime number that is larger than 6? (Difficulty level: 2)

Solution 4.1. Let A be the event of getting a prime number and B be the event of getting an integer larger than 6. $A = \{2, 3, 5, 7, 11\}$ and $B = \{7, 8, 9, 10, 11, 12\}$. The desired outcomes are the elements in both A and B, which is $A \cap B = \{7, 11\}$. So $P(A \cap B\} = \frac{2}{12} = \boxed{\frac{1}{6}}$.

Now, what if we need to find the probability that A or B (or both) happens?

Problem 4.2. Randomly draw an integer from 1 to 12 inclusive. What is the probability that it is a prime number or it is larger than 6 (or both)? (Difficulty level: 3)

Solution 4.2. Let A and B be the events stated above. In this case, we cannot just add the number of elements in A and B together to get the number of desired outcomes because we will be double counting some outcomes, namely '7' and '11', as they appear in both A and B. So we also have to subtract the number of double counted outcomes to get the number of desired outcomes. This is the full **addition rule**, and we can express it as:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

In this case, $|A \cup B| = 5 + 6 - 2 = 9$, so $P(A \cup B) = \frac{9}{12} = \boxed{\frac{3}{4}}$.

The relationship between the probability of the intersection and union of sets is similar:

Theorem 1.4. For any events A, B,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Equivalently, $$P(A \cap B) = P(A) + P(B) - P(A \cup B)$$

To see why, notice that

$$\begin{aligned} P(A) + P(B) - P(A \cap B) &= \frac{|A|}{|\Omega|} + \frac{|B|}{|\Omega|} - \frac{|A \cap B|}{|\Omega|} \\ &= \frac{|A| + |B| - |A \cap B|}{|\Omega|} \\ &= \frac{|A \cup B|}{|\Omega|} \\ &= P(A \cup B) \end{aligned}$$

For the case of more than two events, the relationship is more complicated, and we will talk about it later. Note that in general (for $n \geq 3$),

$$P(A_1 \cup A_2 \cup \ldots \cup A_n) \neq P(A_1) + P(A_2) + \ldots + P(A_n) - P(A_1 \cap A_2 \cap \ldots \cap A_n)$$

Let's try another problem.

Problem 5. When randomly drawing a card from a poker deck, what is the probability of drawing a face card or drawing a card with spades?

(Difficulty level: 3)

Discussion 5. In a poker deck, there are a total of 52 cards. There are 4 suits: tiles $\diamondsuit$, clubs $\clubsuit$, hearts $\heartsuit$, spades $\spadesuit$. Each suit consists of 13 cards, and each of the 13 cards has a different rank. The ranks are A, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K . So a card has a rank and a suit, like $\diamondsuit$3 or $\spadesuit$K. We can see that each rank has 4 cards belonging to different suits. (eg. Rank 3 has the cards $\diamondsuit$3, $\clubsuit$3, $\heartsuit$3, $\spadesuit$3.) Face card are the cards with rank J, Q, K.

Solution 5. Let A be the event drawing a face card, and B be the event drawing a card with spades. $P(A) = \frac{3}{13}$ and $P(B) = \frac{1}{4}$. There are 3 face cards with spades, namely $\spadesuit$J, $\spadesuit$Q, $\spadesuit$K. So $P(A \cap B) = \frac{3}{52}$. $P(A \cup B) = \frac{3}{13} + \frac{1}{4} - \frac{3}{52} = \frac{12+13-3}{52} = \boxed{\frac{11}{26}}$.

1.3 Complement

The **complement** of an event A is the event that A does not happen. It is typically denoted by A'. By definition, A and A' are disjoint and $A \cup A' = \Omega$, that is, A and the complement of A takes up the entire sample space. For example, if A is the event of getting a '6' in a dice throw, then the complement

A' is the event of **not** getting a '6' in a dice throw. We have $A = \{6\}$ and $A' = \{1, 2, 3, 4, 5\}$. If A is the event of getting an even number in a dice throw, then A' is the event of not getting an even number in a dice throw, which is equivalent to getting odd numbers.

The probability of an event and the probability of its complement must add up to 1 , because there is absolute certainty that the outcome of an experiment is in the sample space. Mathematically, we have the **complement rule**:

Theorem 1.5. If A' is the complement of event A, then

$$P(A) + P(A') = 1$$

$$\text{or} \qquad P(A') = 1 - P(A)$$

To verify this mathematically, we have:

$$\begin{aligned} P(A) + P(A') &= \frac{|A|}{|\Omega|} + \frac{|A'|}{|\Omega|} \\ &= \frac{|A| + |A'|}{|\Omega|} \\ &= \frac{|A \cup A'|}{|\Omega|} \\ &= \frac{|\Omega|}{|\Omega|} \\ &= 1 \end{aligned}$$

Problem 6. A bag contains 18 balls. 10 of them are red and the rest of them are blue. Randomly draw a ball from the bag. What is the probability that it is a blue ball?

(Difficulty level: 2)

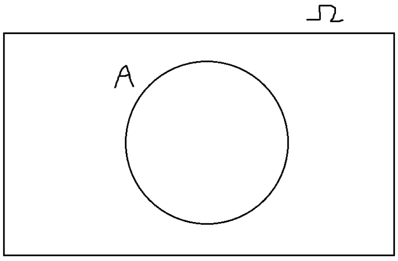
Solution 6.1 The number of blue balls is $18 - 10 = 8$.
So $P(\text{blue ball}) = \frac{8}{18} = \boxed{\frac{4}{9}}$.

Solution 6.2 The probability of drawing a red ball is $\frac{10}{18} = \frac{5}{9}$. The event 'drawing a blue ball' is the complement of the event 'drawing a red ball'. So the probability of drawing a blue ball is $1 - \frac{5}{9} = \boxed{\frac{4}{9}}$.

1.4 Venn diagrams, De Morgan's Laws and distributive laws

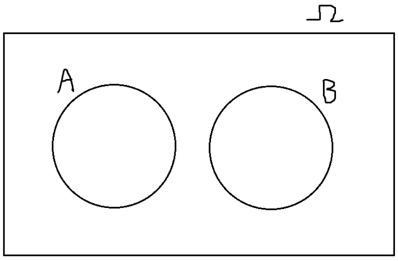
1.4.1 Venn diagrams

We can use **Venn diagrams** to visualize the relation between sets or events. An event A in the sample space Ω can be represented with a Venn diagram:

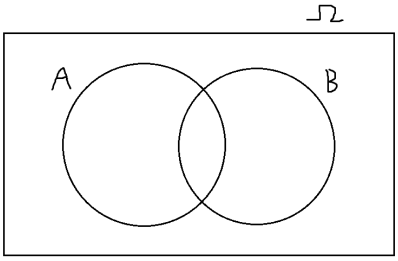


Event A is represented by a circle and the sample space Ω is represented by a rectangle. If an element in the sample space is in set A, then it is inside the circle. If an element in the sample space is not in A, then it is outside the circle but still inside the rectangle.

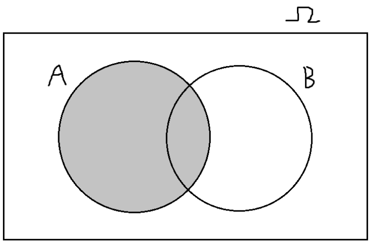
When there are two disjoint events A, B, they can be represented by two separate circles.



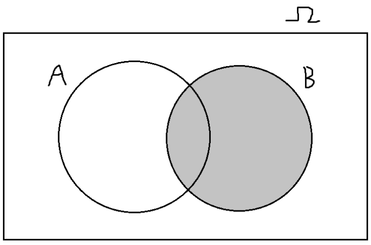
When there are two non-disjoint events A, B, they can be represented by two overlapping circles. The elements that are in both A and B are inside the overlapping region of the circles.



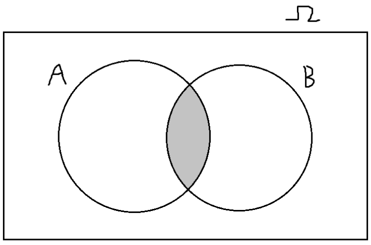
We can represent the events and compound events by the shaded region.



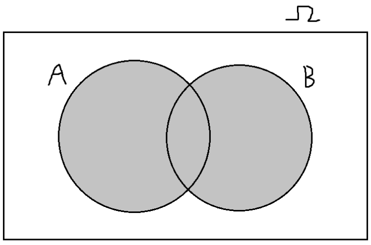
A



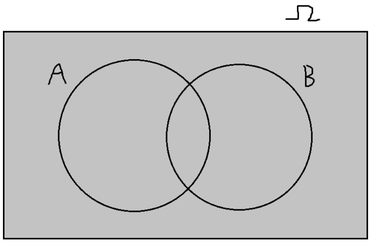
B



$A \cap B$



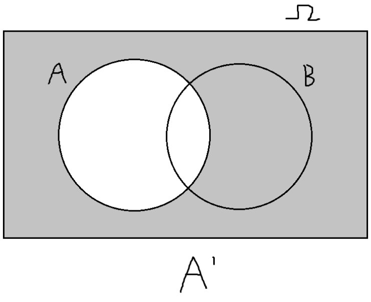
$A \cup B$

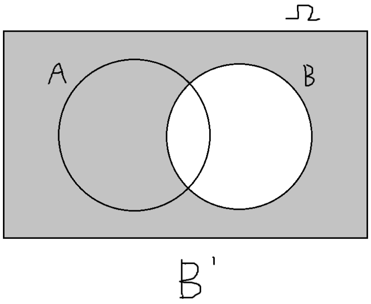


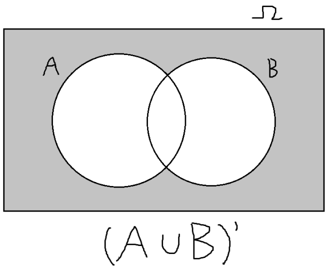
Ω

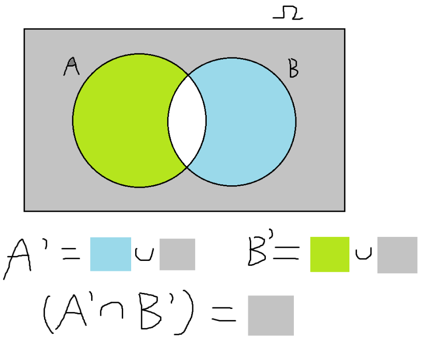
In the Venn diagrams, $A \cap B$ is the common region of A and B, and $A \cup B$ is the total region (without double counting) occupied by A and B.

1.4.2 De Morgan's Laws



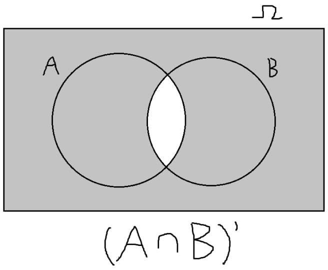


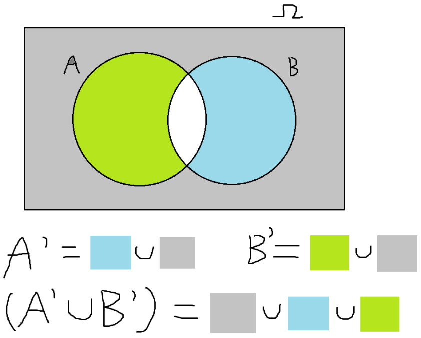




As you can see, $(A \cup B)'$ is the common region of A' and B'. So we have $(A \cup B)' = A' \cap B'$, which is one of the **De Morgan's laws**.

The other De Morgan's Law states $(A \cap B)' = A' \cup B'$.





We can see that the De Morgan's Law is true, because $(A \cap B)'$ is the total region occupied by A' and B' .

Theorem 1.6. The De Morgan's Laws state that

$$(A \cup B)' = A' \cap B'$$

$$(A \cap B)' = A' \cup B'$$

Stated in plain words, if x is neither in A nor in B, then x is not in A and x is not in B. If x is not in both A and B, then x is not in A or x is not in B.

The De Morgan's Laws can be generalized for three or more events. In general, if there are n events labelled $A_1, A_2, \ldots, A_i$, then

$$(A_1 \cup A_2 \cup \ldots \cup A_n)' = A_1' \cap A_2' \cap \ldots \cap A_i'$$
$$(A_1 \cap A_2 \cap \ldots \cap A_n)' = A_1' \cup A_2' \cup \ldots \cup A_i'$$

We can see that if we take the complement of the union/intersection of the events, then we 'distribute' the complement to each event and 'flip' the union/intersection sign.

Notations

We can compact $A_1 \cup A_2 \cup \ldots \cup A_i$ with the big union symbol.

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_i$$

Similarly, we can compact $A_1 \cap A_2 \cap \ldots \cap A_i$ with the big intersection symbol.

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_i$$

The laws can be stated as

$$\left(\bigcup_{i=1}^{n} A_i\right)' = \bigcap_{i=1}^{n}(A_i')$$

$$\left(\bigcap_{i=1}^{n} A_i\right)' = \bigcup_{i=1}^{n}(A_i')$$

Proof of the generalized De Morgan's Laws

We will use **mathematical induction** [4]. First we prove the first law.

For $n = 1$, $\left(\bigcup_{i=1}^{1} A_i\right)'$ and $\bigcap_{i=1}^{1}(A_i')$ is just A' itself, so it is obviously true.

For $n = 2$, $\left(\bigcup_{i=1}^{2} A_i\right)' = \bigcap_{i=1}^{2}(A_i')$ is the regular De Morgan's law, and we have just shown that it is true.

Assume that $\left(\bigcup_{i=1}^{k} A_i\right)' = \bigcap_{i=1}^{k}(A_i')$ is true. Then when $n = k+1$,

$$\begin{aligned}
\text{L.H.S.} &= \left(\bigcup_{i=1}^{k+1} A_i\right)' \\
&= \left[\left(\bigcup_{i=1}^{k} A_i\right) \cup A_{k+1}\right]' \\
&= \left[\bigcup_{i=1}^{k} A_i\right]' \cap A_{k+1}' && \text{(regular De Morgan's Law)} \\
&= \left(\bigcap_{i=1}^{k}(A_i')\right) \cap A_{k+1}' && \text{(Inductive hypothesis)} \\
&= \bigcap_{i=1}^{k+1}(A_i') \\
&= \text{R.H.S.}
\end{aligned}$$

Thus, the statement $(\bigcup_{i=1}^{n} A_i)' = \bigcap_{i=1}^{n}(A_i')$ is true for all positive integers n.

Let's consider the second generalized law.

Similarly, $(\bigcap_{i=1}^{n} A_i)' = \bigcup_{i=1}^{n}(A_i')$ is true for $n = 1, 2$.

Assume that $\left(\bigcap_{i=1}^{k} A_i\right)' = \bigcup_{i=1}^{k}(A_i')$ is true. Then when $n = k+1$,

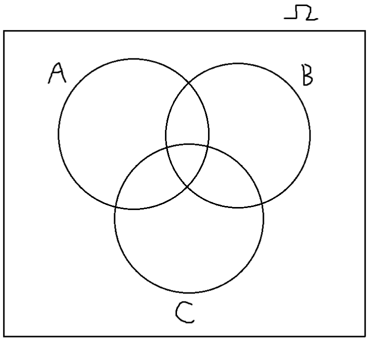
[4] By mathametical induction, when there is a statement or preposition involving n, if we can prove that the statement is true for $n = 1$, and (if the statement is true for an arbitrary integer $n = k$, then it is also true for $n = k + 1$), then the statement is true for all positive integers n .

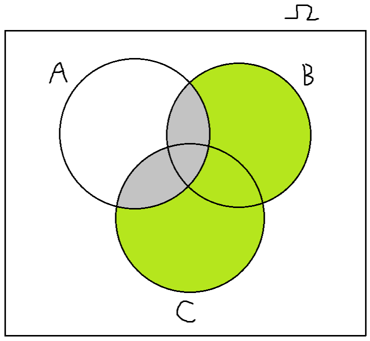
$$
\begin{aligned}
\text{L.H.S.} &= \left(\bigcap_{i=1}^{k+1} A_i\right)' \\
&= \left[\left(\bigcap_{i=1}^{k} A_i\right) \cap A_{k+1}\right]' \\
&= \left[\bigcap_{i=1}^{k} A_i\right]' \cup A'_{k+1} && \text{(regular De Morgan's Law)} \\
&= \left(\bigcup_{i=1}^{k} (A'_i)\right) \cup A'_{k+1} && \text{(Inductive hypothesis)} \\
&= \bigcup_{i=1}^{k+1} (A'_i) \\
&= \text{R.H.S.}
\end{aligned}
$$

Thus, the statement $(\bigcap_{i=1}^{n} A_i)' = \bigcup_{i=1}^{n}(A'_i)$ is true for all positive integers n.

1.4.3 Distributive laws

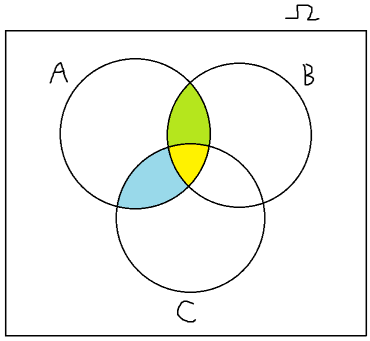
This time, the Venn diagram involves three sets.





$B \cup C =$ ⬜ $\cup$ 🟩

$A \cap (B \cup C) =$ ⬜

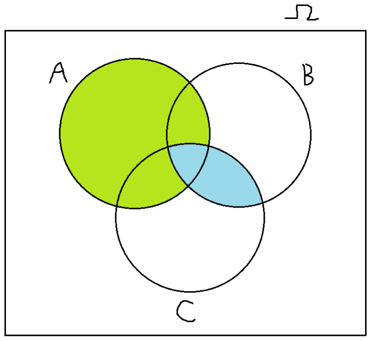


$A \cap B =$ 🟩 $\cup$ 🟨 $A \cap C =$ 🟦 $\cup$ 🟨

$(A \cap B) \cup (A \cap C) =$ 🟩 $\cup$ 🟦 $\cup$ 🟨

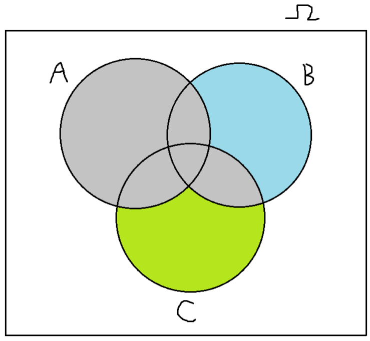
For any sets A, B, C, we can see that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, which is one of the distributive laws.

Another distributive law states that $A \cup (B \cap C) = (A \cup B) \cap (A \cap C)$.



$B \cap C =$ 🟦

$A \cup (B \cap C) =$ 🟩 $\cup$ 🟦



$A \cup B =$ ⬜ $\cup$ 🟦 $A \cup C =$ ⬜ $\cup$ 🟩

$(A \cup B) \cap (A \cup C) =$ ⬜

We can see that it is also true.

Theorem 1.7. The distributive laws state that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cap C)$$

Stated in plain words, if x is in A and x is in B or C, then x is in both A and B or x is in both B or C.

Similarly, if x is in A or x is in both B and C, then x is in A or B, and x is in A or C.

This law can be extended to more events. In general, if there are there are n events labelled B_1, B_2, ... , B_n, , then for any event A we have

$$\begin{aligned} A \cap \left(\bigcup_{i=1}^{n} B_i \right) &= \bigcup_{i=1}^{n} (A \cap B_i) \\ A \cup \left(\bigcap_{i=1}^{n} B_i \right) &= \bigcap_{i=1}^{n} (A \cup B_i) \end{aligned}$$

The proof is similar. For the first law, we know that the statement is true for n=1, 2. Assume that $A \cap \left(\bigcup_{i=1}^{k} B_i \right) = \bigcup_{i=1}^{k} (A \cap B_i)$ is true. When $n = k + 1$,

$$\begin{aligned} \text{LHS} &= A \cap \left(\left(\bigcup_{i=1}^{k} B_i \right) \cup B_{k+1} \right) \\ &= \left(A \cap \left(\bigcup_{i=1}^{k} B_i \right) \right) \cup (A \cap B_{k+1}) && \text{(regular distributive law)} \\ &= \left(\bigcup_{i=1}^{k} (A \cap B_i) \right) \cup (A \cap B_{k+1}) && \text{(inductive hypothesis)} \\ &= \bigcup_{i=1}^{k+1} (A \cap B_i) \\ &= \text{RHS} \end{aligned}$$

By mathematical induction, $A \cap (\bigcup_{i=1}^{n} B_i) = \bigcup_{i=1}^{n} (A \cap B_i)$ is true for all positive integers n.

For the second law, we know that the statement is true for n=1, 2. Assume that $A \cup \left(\bigcap_{i=1}^{k} B_i\right) = \bigcap_{i=1}^{k}(A \cap B_i)$ is true. When $n = k + 1$,

$$\begin{aligned}
\text{LHS} &= A \cup \left(\left(\bigcap_{i=1}^{k} B_i\right) \cap B_{k+1}\right) \\
&= \left(A \cup \left(\bigcap_{i=1}^{k} B_i\right)\right) \cap (A \cup B_{k+1}) && \text{(regular distributive law)} \\
&= \left(\bigcap_{i=1}^{k}(A \cup B_i)\right) \cap (A \cup B_{k+1}) && \text{(inductive hypothesis)} \\
&= \bigcap_{i=1}^{k+1}(A \cup B_i) \\
&= \text{RHS}
\end{aligned}$$

By mathematical induction, $A \cup (\bigcap_{i=1}^{n} B_i) = \bigcap_{i=1}^{n}(A \cup B_i)$ is true for all positive integers n.

1.5 Probability distribution

So far, we have been talking about experiments with outcomes of uniform probability, but there can be experiments with outcomes of uneven (non-uniform) probability, such as flipping a **biased** coin that has a $\frac{3}{4}$ probability of landing on a head, and $\frac{1}{4}$ probability of landing on a tail. The sample space is still {H, T} , but the probability is distributed differently into each outcome. We may also want to consider how probability is distributed into different (disjoint) events. That's where probability distribution comes in.

Probability distribution is a mathematical **function** that describes the probability of each individual outcomes or some events in an experiment. It takes in an outcome or event as input and outputs a value between 0 and 1 (inclusive) known as the probability (of that input). A probability distribution that takes in an outcome x is denoted $P(x)$, and an event A as input is $P(A)$ (as we have seen before). (When we are talking about probability of event A, we are talking about $P(A)$, but probability distribution is just what we call the function P itself, so it is not really a new concept.)

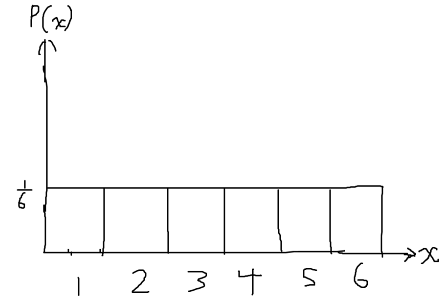
By viewing probability distribution as a function[5] , a probability distribution that only takes in outcomes in the sample space Ω can be writ-

[5] Recall the definition of a function: A function f from set X to set Y assigns to each $x \in X$, exactly one element $f(x) \in Y$. X is called the **domain** and Y is called the **codomain**. It can be written as $f : X \to Y$.

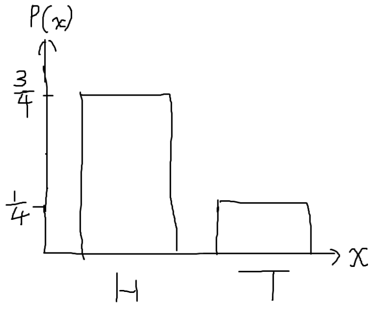
ten as $P : \Omega \to [0, 1]$, where $[0, 1]$ is the set (interval) of all real numbers between 0 and 1 inclusive. If there is a probability distribution that only takes in n events denoted by $A_1, A_2, \ldots, A_n$, then it can be written as $P : \{A_1, A_2, \ldots, A_n\} \to [0, 1]$.

Right now, we are talking about **discrete** probability distribution, in which the domain of the function has finite (or countably infinite) elements. It means that there are finite (/countably infinite) amount of outcomes or events to take as inputs. Discrete probability distribution is also called **probability mass function**.

Now let's consider the probability distribution of a sample space (i.e. its domain is the sample space and it only takes in outcomes as its input). There are different types of probability distributions, and the one we talked about in section 1.1 is a **uniform** probability distribution. It means that every outcome in the sample space has an equal probability of occurring. Let's consider the example of throwing a fair dice. We can visualize the probability distribution using a **bar graph**:

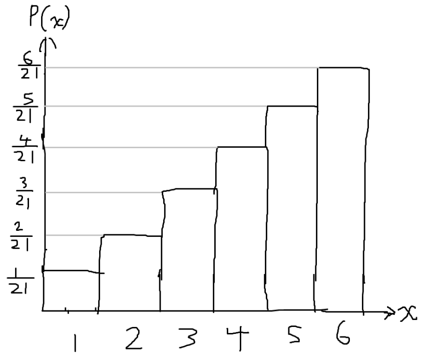


There can also be uneven probability distribution. Consider the probability distribution of the biased coin mentioned above:



What if we need to find the probability of an event with multiple desired outcomes in an uneven probability distribution?

Problem 7. Imagine that there is a 'magic dice' with uneven probability distribution as follows:



When throwing the magic dice, what is the probability of getting '3' or smaller?

(Difficulty level: 2)

Solution 7. We can consider that there are three events, each consisting of a different outcome, namely $\{1\}$, $\{2\}$, $\{3\}$. What we are trying to find is the probability of their union $\{1\} \cup \{2\} \cup \{3\}$. Since they are disjoint, we can sum their probabilities together to get the required probability $P(\{1\} \cup \{2\} \cup \{3\}) = \frac{1}{21} + \frac{2}{21} + \frac{3}{21} = \boxed{\frac{2}{7}}$.

Discussion 7. If we use the formula $P(A) = \frac{\text{Number of desired outcomes}}{\text{Number of possible outcomes}}$, we will get the wrong answer $\frac{1}{2}$. We can see that the formula no longer works in uneven probability distribution, so we need to make sure that the probability distribution of a sample space is even (uniform) before using the formula.

Note that if we were to throw the dice many many times (like a trillion times), the **relative frequency**[6] of the outcomes will approach the probability distribution, that is, the ratio of their frequencies (number of occurrences) will be very close to the ratio of their probabilities.

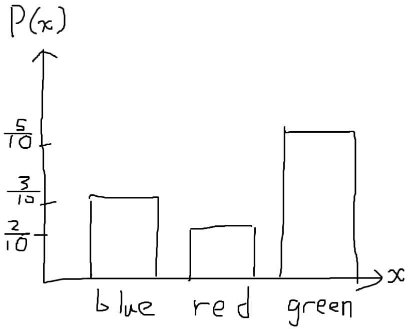
In general, the probability that the outcome of an experiment is one of the n outcomes labelled $x_1, x_2, \ldots, x_n$, is equal to the sum of their individual probabilities. We can express it as:

$$P(\{x_1\} \cup \{x_2\} \cup \ldots \cup \{x_n\}) = P(\{x_1\}) + P(\{x_2\}) + \ldots + P(\{x_n\})$$

We can also define probability distribution with regard to events, such as drawing each colour of balls from a bag of balls.

[6] relative frequency $= \frac{\text{Number of times something occurs}}{\text{Total number of trials}}$

If there are 10 balls in a bag, in which there are 3 blue balls, 2 red balls and 5 green balls. Then if I randomly (uniformly random) draw a ball from the bag, the probability distribution with regard to the colour of the balls is



1.6 Independent events

Two events are **independent** (of each other) if knowing that one event happens does not affect the probability that the other event happens. An example is flipping a coin two times. If we know the first coin flip is a head, it will not affect the probability that the second coin flip is a head (or a tail). The probability is still $\frac{1}{2}$. The same is true for dice throws. If we know the first throw is a '6', it will not affect the probability of the second throw being a '6'. A more counter-intuitive example is that in a dice throw, if we know that the number we get is an even number, it does not affect the probability that it is divisible by 3, and vice versa.

The probability that A happens **given** that B has happened is denoted by $P(A|B)$, and when A, B are independent, we have $P(A|B) = P(A)$ and $P(B|A) = P(B)$.

Besides events, there can also be independent experiments or independent trials. For an experiment with two independent trials, the fact that the first trial has conducted, or whatever the outcome is, does not change the probability distribution of the second trial (/probability distribution of the sample space). Similarly, if there are two independent (and different) experiments, the fact that one has been conducted, or whatever the outcome is, does not change the probability distribution of the second experiment. For example, getting a head in a coin flip will not change the probability of getting a '6' or any other outcomes in a dice throw.

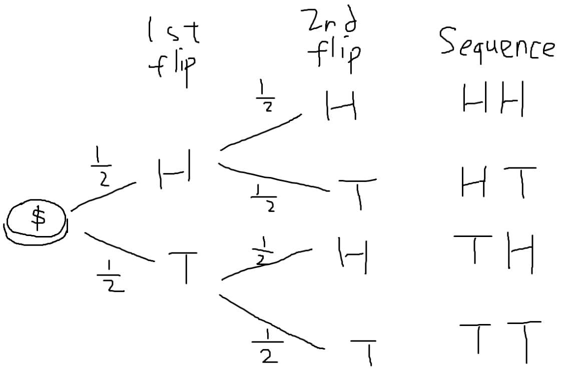
Two different experiments are generally considered to be independent unless stated otherwise. For the case of an experiment with multiple trials, whether the trials are independent depends on the nature of the experiment or is there any differences in the sample space of each individual trial. Multiple coin flips and multiple dice throws are the example of independent trials. As for the example of not independent (/dependent) trials, when drawing two balls from a bag **without replacement**, the first trial (draw) and the second trial (draw) is not independent (/is dependent), since the sample space in the 2nd trial is reduced by one element (i.e. the ball drawn in the 1st trial).

1.6.1 Intersection of two independent events

What if we want to know the probability of both two independent events happening in two trials, such as the probability of getting two heads in two coin flips? First, let's consider all the possible sequences using a table. (The sample space of two coin flips)

	1st throw is H	1st throw is T
2nd throw is H	HH	TH
2nd throw is T	HT	TT

Alternatively, we can use a **tree diagram** to show the possible sequences.



As you can see, there are 4 possible sequences, so the sample space is {HH, TH, HT, TT}. Note that the sample space of **two** coin flips is **not** the sample space of an individual coin flip {H, T}. Each sequence is the outcome of two coin flips, and there are a total of $2 \cdot 2 = 4$ outcomes. Each outcome is equally likely, with a probability of $\frac{1}{4}$, because the two coin flips are independent, so when half the times the first flip is H, in half of that 'half of the times' will the second flip be H, as shown in the tree diagram. When there is half of half something, we get one quarter $(\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4})$. The same can be said for other outcomes. The desired outcome is HH, and so it has a probability of $\frac{1}{4}$.

What if we want to find the probability of getting one head and one tails? In this case, what order H and T occur does not matter to us, and there are two possible orders, 'HT' and 'TH', which are the desired outcomes. So the probability is $\frac{2}{4} = \frac{1}{2}$.

What if we want to find the probability of getting **at least** one heads? In this case, the number of heads can be one or two, and there are three outcomes: 'HT', 'TH', 'HH', so it has the probability of $\frac{3}{4}$.

Let's consider another example.

Problem 8. A fair dice is thrown and a fair coin is flipped independently. What is the probability that the dice lands on '6' and the coin lands on 'H'?

(Difficulty level: 3)

Discussion 8. You may think that since we do not know the order that the two experiments are conducted, we cannot know the answer. But actually, the order of the experiments does not matter. They may even be conducted at the same time, for all we know. Since the two experiments are independent, whether one experiment has been conducted, has not yet been conducted or is ongoing, does not affect the probability distribution of another experiment.

The sample space of the dice throw Ω_{dice} is $\{1, 2, 3, 4, 5, 6\}$, and the sample space of the coin flip Ω_{coin} is $\{\text{H, T}\}$. However, we cannot consider the sample spaces of the two experiments separately, because we are finding the intersection of two events in two different experiments (getting a '6' in a 6-sided dice throw and getting a '1' in a 4-sided dice throw). If we only consider the sample space of a single experiment, we are neglecting the event happening in another experiment. So the possible outcomes of two experiments are all possible combinations of outcomes of each individual experiment, which is the **set product/ Cartesian product** [7] of the two sample spaces.

We can draw a table to show all possible outcomes (sample space) of the two experiments.

Dice Coin	1	2	3	4	5	6
H	H, 1	H, 2	H, 3	H, 4	H, 5	H, 6
T	T, 1	T, 2	T, 3	T, 4	T, 5	T, 6

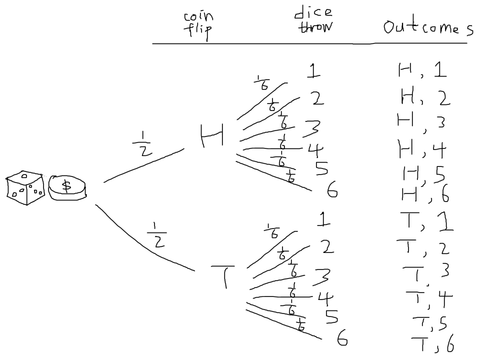
Whether we write 'H, 1' or '1, H' does not matter, and it means the same thing, since there is only one way that 'H' and '1' both occur.

[7] The set product of two sets A and B, denoted $A \times B$, is the set of all ordered pairs (a, b) where a is in A and b is in B.

Alternatively, we can express the sample space as a set product
$\Omega_{coin} \times \Omega_{dice}$ ={(H, 1), (H, 2), (H, 3), (H, 4), (H, 5), (H, 6),
. (T, 1), (T, 2), (T, 3), (T, 4), (T, 5), (T, 6)}

(or $\Omega_{dice} \times \Omega_{coin}$, which has the same combination of outcomes)

We can see that the total number of possible outcomes is $|\Omega_{coin}| \times |\Omega_{dice}| = 2 \times 6 = 12$. Each of the outcomes has an equal probability of occurring (even though $P(\text{H}) \neq P(1)$), since both sample spaces have even probability distribution. To understand this, consider that when half of the time that H occurs in a coin flip, in $\frac{1}{6}$ of the time will '6' occur in a dice throw. The same can be said for all other outcomes. We can draw a tree diagram to illustrate this.



Solution 8. Therefore, the probability of an outcome is $\frac{1}{2} \times \frac{1}{6} = \frac{1}{12}$. Since there is only one desired outcome, $P(\text{H,6}) = \boxed{\frac{1}{12}}$

For experiments with uniform probability distributions, in general, if there are two independent experiments/trials each with M and N possible outcomes, there are a total of MN possible outcomes for the two experiments. This is the **multiplication principle**. The probability that a particular combination of outcome occurs is $\frac{1}{MN}$.

This can be extended to three or more experiments/trials. If there are n independent experiments/trials each with $N_1, N_2, \ldots, N_n$ possible outcomes, then the probability that a particular combination of outcome occurs is $\frac{1}{N_1 N_2 \ldots N_n}$. Similarly, if there is an experiment such that x is one of the N possible outcomes, and there are n independent trials of the experiment, the probability that x occurs for n times is $(\frac{1}{N})^n$

Problem 9. When a fair dice is thrown three times, what is the probability that all of the numbers thrown are '6'?

(Difficulty level: 3)

Discussion 9. We may list out all of the possible outcomes for three dice throws but we will find that it is too troublesome. Actually, when we know the probability of an outcome in a single trial, we can quickly calculate the probability of multiple trials.

Solution 9. The probability of getting a ‘6’ in a single dice throw is $\frac{1}{6}$, so the probability of getting ‘6’ in all three dice throws is $(\frac{1}{6})^3 = \boxed{\frac{1}{216}}$.

Now, what if each individual experiment has more than one desired outcomes?

Problem 10. A fair dice is thrown and a card is randomly drawn from a poker deck. What is the probability that the dice lands on a square number and the card drawn is not a spade?

(Difficulty level: 3)

Discussion 10. We may list out all of the possible outcomes, but there are $52 \times 6 = 312$ outcomes, so it is too troublesome. However, we can simplify the sample space for the poker cards to only 4 suits, since each suit has a equal number of cards, and we don’t care about what specific card is drawn but only the suits.

Solution 10a. We can list out all the possible combinations using a table.

Dice Card	1	2	3	4	5	6
♢	♢, 1	♢, 2	♢, 3	♢, 4	♢, 5	♢, 6
♧	♧, 1	♧, 2	♧, 3	♧, 4	♧, 5	♧, 6
♡	♡, 1	♡, 2	♡, 3	♡, 4	♡, 5	♡, 6
♤	♤, 1	♤, 2	♤, 3	♤, 4	♤, 5	♤, 6

For the dice throw, the desired outcomes are ‘1’ and ‘4’, and for the card draw, the desired outcomes are ♢, ♧, and ♡. The outcomes that satisfy both requirements are shaded.

Dice Card	**1**	2	3	**4**	5	6
♢	**♢, 1**	♢, 2	♢, 3	**♢, 4**	♢, 5	♢, 6
♧	**♧, 1**	♧, 2	♧, 3	**♧, 4**	♧, 5	♧, 6
♡	**♡, 1**	♡, 2	♡, 3	**♡, 4**	♡, 5	♡, 6
♤	♤, 1	♤, 2	♤, 3	♤, 4	♤, 5	♤, 6

Required probability $= \frac{6}{24} = \boxed{\frac{1}{4}}$.

Solution 10b. Let A be the event of getting a square number in the dice throw, and B be the event of not getting a spade in the card draw. $P(A) = \frac{2}{6} = \frac{1}{3}$ and $P(B) = 1 - \frac{3}{4} = \frac{3}{4}$. Note that A and B are independent. In the table above, note that the fraction of shaded cells in each row of $\{\diamondsuit, \clubsuit, \heartsuit\}$ is $P(A)$ and the fraction of shaded cells in each column of $\{1, 4\}$ is $P(B)$. So $P(A \cap B) = P(A) \cdot P(B) = \frac{1}{3} \cdot \frac{3}{4} = \boxed{\frac{1}{4}}$.

In general, we have the **multiplication rule for independent events**:

Theorem 1.8. Iff A, B are independent events, then

$$P(A \cap B) = P(A) \cdot P(B)$$

To see why, consider that regardless of whether A and B are independent, $P(A \cap B) = P(A) \cdot P(B|A)$, that is, in $P(A)$ of the times, A happens , and in that $P(A)$ of the times that A has happened, B also happens. Since A and B are independent, $P(B) = P(B|A)$, so $P(A \cap B) = P(A) \cdot P(B)$. (A and B can swap places for the argument)

But why $P(A \cap B) = P(A) \cdot P(B|A)$? You may wonder. This involves the nature of randomness. Let there be event A, B that can happen in an experiment. Hypothetically, if the experiment was repeated many many times, say M times, where M is a very large number, larger than any number you can think of. Then the number of times A happens is roughly $P(A) \cdot M$, because the meaning of $P(A)$ is $\frac{\text{Number of times } A \text{ happens}}{M}$. $P(A) \cdot M$ is still a very large number (If $P(A)$ is extremely small, comparable to $\frac{1}{M}$, then just choose a new $M = (1/P(A))^{(1/P(A))}$ or whatever. The meaning of $P(B|A)$ is $\frac{\text{Number of times } B \text{ happens given } A \text{ happens}}{\text{Number of trials in which } A \text{ happens}}$, so in all the $P(A) \cdot M$ trials in which A has happened, the number of times B has happened must be roughly $P(B|A) \cdot (P(A) \cdot M)$, because $P(A) \cdot M$ is still a very large number. As $P(B|A) \cdot (P(A) \cdot M)$ is the number of trials in which both A and B happen, the probability $P(A \cap B)$ is $\frac{P(B|A) \cdot (P(A) \cdot M)}{M} = P(A) \cdot P(B|A)$.

Conversely, if A, B are events such that $P(A \cap B) = P(A) \cdot P(B)$, then A and B must be independent. It is because $P(A \cap B) = P(A) \cdot P(B|A)$ for any A, B, and we assumed above that $P(A \cap B) = P(A) \cdot P(B)$, so $P(A) \cdot P(B) = P(A) \cdot P(B|A)$, giving $P(B) = P(B|A)$. By similar argument, $P(A) = P(A|B)$. (We don't consider events with 0 probability here.)

Thus, the statements $P(A) = P(A|B)$ and $P(A \cap B) = P(A) \cdot P(B)$ are **logically equivalent** [8].

[8] For two logically equivalent statements P, Q, P is true if and only if Q is true

Multiplication rule for more than two independent events

The multiplication rule holds true for more than two independent events. In general, if there are n independent events labelled $A_1, A_2, \ldots, A_n$, then

$$P(A_1 \cap A_2 \cap \ldots \cap A_n) = P(A_1) \cdot P(A_2) \cdot \ldots \cdot P(A_n)$$

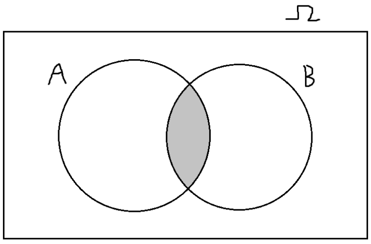
This can be applied when there are multiple trials of the same experiment.

Theorem 1.9. If there are n independent trials of an experiment, and A is an event of a trial, then the probablility that A happens n times is $(P(A))^n$.

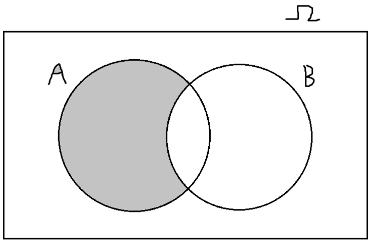
1.6.2 Complements of two independent events

If A, B are independent events, are their complements independent too? Short answer: yes. Long answer: Recall the meaning of independence. If B happens, the probability that A happens remains the same.

This also means that if B does not happen, the probability that A happens must also remain the same. To see why, note that $A \cap B$ and $A \cap B'$ are disjoint. We can show this with a Venn diagram:



$A \cap B$



$A \cap B'$

We can see that $A = (A \cap B) \cup (A \cap B')$. It follows that

$$P(A) = P(A \cap B) + (A \cap B')$$

by the simple addition rule. As A and B are independent, we know that

$$P(A \cap B) = P(A) \cdot P(B)$$

(abbreviated as iff Q). This means if P is true, then Q is true; and if Q is true, then P is true.

. Combining these two equalities, we get

$$\begin{aligned} P(A \cap B') &= P(A) - P(A \cap B) \\ &= P(A) - P(A) \cdot P(B) \qquad \text{(independence of } A.\ B\text{)} \\ &= P(A) \cdot (1 - P(B)) \end{aligned}$$

Since $P(B') = 1 - P(B)$, we obtain the equality

$$P(A \cap B') = P(A) \cdot P(B')$$

, which implies that A and B' are independent.

Using similar reasoning, it follows that

$$P(A' \cap B) = P(A') \cdot P(B)$$

and

$$P(A' \cap B') = P(A') \cdot P(B')$$

.

Thus, we have the conclusion:

Theorem 1.10. if A and B are independent events, then the following pairs are also independent events: A' and B ; A and B' ; A' and B' .

Note that A and A' are never independent events, since if we know that A has happened, then A' will never happen, and $P(A'|A) = 0$.

Problem 11. A bag contains 5 red balls, 7 blue balls and 8 green balls. Randomly draw 4 balls from the bag **with replacements**. What is the probability that all of the balls drawn are blue balls and green balls (or only blue balls or only green balls)?

(Difficulty level: 4)

Discussion 11. The term 'with replacements' means that after a person draws a ball from the bag, they put into the bag another ball that is the same colour as the ball drawn. This is done immediately after each trial, so the sample space of each individual trial is the same. Therefore, we can regard the 4 trials as independent.

Solution 11. Let A be the event 'drawing a blue ball or a green ball' in one trial. $P(A) = \frac{7+8}{5+7+8} = \frac{3}{4}$. Since there are 4 independent trials, $P(\text{all blue and green balls}) = (\frac{3}{4})^4 = \boxed{\frac{81}{256}}$.

Let's try another version of problem 9.

Problem 12. When a fair dice is thrown three times, what is the probability that at least one of the numbers thrown are '6'?

(Difficulty level: 4)

Discussion 12. The desired number of '6' thrown is 1, 2, and 3. We may find the number of outcomes for each case but it is a bit complicated. Instead, we can use find the probability that none of the numbers thrown are '6', then use complement rule to get the answer. This can simplify the calculation.

But why does this work? Let A_n be the event "getting a '6' in the n th trial". Then the event "getting at least one '6' in n trials" is $A_1 \cup A_2 \cup \ldots \cup A_n$. Recall the generalized De Morgan's Law (in Section 1.4)

$$(A_1 \cup A_2 \cup \ldots \cup A_n)' = A_1' \cap A_2' \cap \ldots \cap A_i'$$

. Thus we can write

$$\begin{aligned} P(A_1 \cup A_2 \cup \ldots \cup A_n) &= 1 - P((A_1 \cup A_2 \cup \ldots \cup A_n)') \\ &= 1 - P(A_1' \cap A_2' \cap \ldots \cap A_n') \\ &= 1 - P(A_1') \cdot P(A_2') \ldots \cdot P(A_i') \\ &\quad \text{(since all the } A_i \text{ are independent)} \\ &= 1 - (1 - P(A_1))(1 - P(A_2)) \ldots (1 - P(A_n)) \end{aligned}$$

As the probability of each A_i is the same, we have
$P(\text{at least one '6'}) = 1 - (1 - P(A_1))^n$.

Solution 12. The probability of **not** getting a '6' in a single dice throw is $1 - \frac{1}{6} = \frac{5}{6}$, so the probability of getting no '6' in all three dice throws is $(\frac{5}{6})^3 = \frac{125}{216}$. Thus, the probability of getting at least one '6' is $1 - \frac{125}{216} = \boxed{\frac{91}{216}}$.

Now we can finally tackle the perplexing wither skeleton problem.

Problem 13. In Minecraft, when a wither skeleton is killed, it has a $\frac{1}{40}$ chance of dropping a wither skeleton skull. What is the probability of getting no wither skeleton skulls after killing 100 wither skeletons? (Express the answer in decimal form, correct to three significant figures.)

(Difficulty level: 4)

Solution 13. The probability of not getting a wither skeleton skull is $\frac{39}{40}$. So the probability of getting no wither skeleton skulls in 100 trials is $(\frac{39}{40})^{100} = \boxed{0.0795}$

Discussion 13. As you can see, there is only about 8% chance of this happening, so I was incredibly unlucky that time.

What if we need to find how many trials to be conducted?

Problem 14. How many throws of a fair dice do we need (at least) in order to have a less than $\frac{1}{2}$ chance of at least one '6'?

(Difficulty level: 5) [2] (Classic Problems of Probability Q1)

Solution 14. Let n be the required number of throws. We have $P(\text{at least one '6'}) = 1 - P(\text{no '6'}) = 1 - (\frac{5}{6})^n$. Put

$$\begin{aligned}
1 - (\frac{5}{6})^n &< \frac{1}{2} \\
(\frac{5}{6})^n &> \frac{1}{2} \\
n \cdot \log(\frac{5}{6}) &> \log\frac{1}{2} \\
n &> \frac{\log\frac{1}{2}}{\log(\frac{5}{6})} \\
n &> 3.80 \qquad \text{(cor. to 3 sig. fig.)}
\end{aligned}$$

Therefore we get $n = \boxed{4}$.

1.6.3 Multiple desired outcomes

How about when there are multiple desired outcomes in the sample space of two experiments?

Problem 15. Throw a 6-sided fair dice and a 4-sided fair dice independently. What is the probability that the sum of the numbers thrown is 7 or more?

(Difficulty level: 4)

Discussion 15. Let's draw a table to show all the possible outcomes of the dice throws.

6-sided 4-sided	1	2	3	4	5	6
1	1, 1	1, 2	1, 3	1, 4	1, 5	1, 6
2	2, 1	2, 2	2, 3	2, 4	2, 5	2, 6
3	3, 1	3, 2	3, 3	3, 4	3, 5	3, 6
4	4, 1	4, 2	4, 3	4, 4	4, 5	4, 6

Note that (1, 2) and (2, 1) are different outcomes. To see why, replace the sample space of the 4-sided dice with poker suits like the table Solution 10a. You wouldn't say that (◇, 2) is the same as (♧, 1). This time, it just so happens that some of the outcomes of the 4-sided dice is called the same name as some of the outcomes of the 6-sided dice , and we can do an operation called addition to the two outcomes. (If ◇+2 was defined, we can add the outcomes together too.)

So why is (1, 1) only counted once? Replace it with poker suits. We can see that (◇, 1) and (1, ◇) mean the same thing, and account for the same outcome (since there is only one way both ◇and 1 occur).

Solution 15. Let's calculate the sum for all possible outcomes.

Sum of results of two dice throws

6-sided 4-sided	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10

The shaded cells are the desired outcomes and there are 10 of them. So P(sum is 7)= $\frac{10}{24} = \boxed{\frac{5}{12}}$.

Problem 16. A coin is flipped three times. What is the probability of getting exactly 2 heads and 1 tail?

(Difficulty level: 4)

Solution 16 We can list all possible outcomes for three coin flips since there are only 8 possible outcomes in total:

{ HHH, HHT, HTH, HTT, THH, THT, TTH, TTT }

There are 3 desired outcomes: HHT, HTH, THH. So
P(2 heads, 1 tail)= $\boxed{\frac{3}{8}}$.

Problem 17. Two players A and B play a fair game (both players have equal chance of winning each round) such that the player who wins a total of 6 rounds first wins a prize. Suppose that A has won a total of 5 rounds and B has won a total of 3 rounds. What is the probability that A wins the prize?

(Difficulty level: 4) [2] (Classic Problems of Probability Q4)

Solution 17. Let's assume that the players do not immediate stop playing after one of them wins the prize. Also note that for the next 3 rounds, one of them must win the prize in one of the rounds. For these next 3 rounds, the set of possible sequences of players who win the game is {AAA, AAB, ABA, ABB, BAA, BAB, BBA, BBB}.

In the 8 equally likely outcomes, only one of them (BBB) will result in player B winning. So $P(A \text{ wins the prize}) = \boxed{\frac{7}{8}}$

1.6.4 Union of two independent events

What if we want to know the probability of either one (or both) of the two independent events happening in two trials?

For independent events A, B, when we know their individual probabilities, we can calculate the probability of their intersection. Then we can also know the probability of their union. Recall the addition rule:
For any events A, B, $\quad P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

If A, B are independent, then $P(A \cap B) = P(A) \cdot P(B)$.

Thus, we have $P(A \cup B) = P(A) + P(B) - P(A) \cdot P(B)$.

Problem 18. In each week, Alan will randomly choose a day (with uniform probability) to throw a 4-sided fair dice. In a particular week, what is the probability that the dice is thrown on a weekend **or** the number thrown is a '4' (or both)?

(Difficulty level: 4)

Solution 18a. Let's draw a table to show all the possible outcomes, and shade the desired outcomes.

Day Dice	Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	Mon, 1	Tue, 1	Wed, 1	Thu, 1	Fri, 1	Sat, 1	Sun, 1
2	Mon, 2	Tue, 2	Wed, 2	Thu, 2	Fri, 2	Sat, 2	Sun, 2
3	Mon, 3	Tue, 3	Wed, 3	Thu, 3	Fri, 3	Sat, 3	Sun, 3
4	Mon, 4	Tue, 4	Wed, 4	Thu, 4	Fri, 4	Sat, 4	Sun, 4

The number of desired outcomes is 13, so $P(\text{weekend or `4'}) = \boxed{\frac{13}{28}}$.

Solution 18b. Let A be the event of throwing the dice on a weekend, and B be the event of getting a '4' in a dice throw. $P(A) = \frac{2}{7}$ and $P(B) = \frac{1}{4}$. Since A and B are independent, $P(A \cup B) = P(A) + P(B) - P(A) \cdot P(B)$ $= \frac{2}{7} + \frac{1}{4} - (\frac{2}{7})(\frac{1}{4}) = \boxed{\frac{13}{28}}$.

Solution 18c. We can first find the probability that the dice is not thrown on a weekend **and** the number thrown is not a '4', then take the complement of that to get the answer. This works because of De Morgan's law: $A \cup B = (A' \cap B')'$. Thus,

$$\begin{aligned} P(A \cup B) &= P((A' \cap B')') \\ &= 1 - P(A' \cap B') \\ &= 1 - (1 - P(A))(1 - P(B)). \end{aligned}$$

Let A, B be the events stated above. We have
$P(A \cup B) = 1 - (1 - \frac{2}{7})(1 - \frac{1}{4}) = 1 - (\frac{5}{7})(\frac{3}{4}) = \boxed{\frac{13}{28}}$.

1.7 Dependent events

Sometimes two events are not independent (/are dependent), and knowing one event happens changes the probability that the other event happens. For example, when throwing a dice, let A be the event of getting a prime number, and let B be the event of getting an even number. Individually, $P(A) = \frac{1}{2}$ and $P(B) = \frac{1}{2}$. However, if we know that A happens, meaning the number thrown is a prime, the probability of B (getting an even number) changes to $\frac{1}{3}$. We write that $P(B|A) = \frac{1}{3}$. In general, for two dependent events, $P(B) \neq P(B|A)$ and $P(A) \neq P(A|B)$.

Two trials of an experiment can be dependent. As stated earlier, if we conduct an experiment of drawing a ball from the bag without replacements, then the trials of the experiment are dependent because each time, we remove a ball from the sample space. Which element is removed in the sample space of the second trial depends on the outcome of the first trial. So the probabilities of some events in the second trial are changed as well.

If we need to find the intersection of two dependent events, we have the **general multiplication rule** (discussed in Section 1.6.1):

Theorem 1.11. For any events A, B,

$$P(A \cap B) = P(A) \cdot P(B|A)$$

$$P(A \cap B) = P(B) \cdot P(A|B)$$

This holds true regardless of whether A, B are independent. But in the case that A, B, are independent, we will simply write $P(B)$ instead of $P(B|A)$, so this formula is usually used for dependent evennts.

1.7.1 Conditional independence

Sometimes, given that C has happened, A and B becomes independent. However A and B are dependent if C does not happen. We call A and B **conditionally independent**.

Suppose there are a total of 7 balls in a bag, and exactly 4 of them are blue balls. The blue balls are labelled ‘1’, ‘2’, ‘3’, ‘4’ each. I randomly draw two balls from the bag without replacement. Let A be the event of drawing blue ball ‘1’ in the first draw, and B be the event of drawing a blue ball in the second draw. C is the event of drawing a blue ball in the first draw.

Given that C has happened (i.e. the first draw is a blue ball), $P(B|C) = \frac{3}{6}$. If A has also happened (the first draw is blue ball ‘1’), $P(B|A, C) = \frac{3}{6}$ stays the same. This is because after a blue ball is drawn, no matter which blue ball, the number of blue balls remaining is 3 and the total number of balls remaining is 6. Therefore A, B are conditional independent given C happens, that is, given that the first draw is a blue ball, the probability that the second draw is also a blue ball is independent of which blue ball is drawn. This concept can be used to solve problems involving drawing balls from a bag without replacement.

However, A and B are dependent. If given that A happens (blue ball ‘1’ is drawn), $P(B|A) = \frac{3}{6}$. If given that A does not happen (blue ball ‘1’ is not drawn), the sample space of the first draw is reduced to 6 balls in total,

in which there are 3 blue balls. It is not certain which ball is drawn. Half the time it can be blue. Half the time it can be not blue, and the probability distribution (with regard to colour of balls) of the 2nd draw depends on the outcome of the 1st draw.
$P(B|A') = (\frac{1}{2})(\frac{3}{6}) + (\frac{1}{2})(\frac{4}{6}) = \frac{7}{12} \neq P(B|A)$

Lastly, if we do not know whether A happens:
$P(B) = (\frac{4}{7})(\frac{3}{6}) + (\frac{3}{7})(\frac{4}{6}) = \frac{4}{7} \neq P(B|A)$

Let's see if the multiplicative rule for independent events works for A, B if C has happened.

$$P(A|C) = \frac{1}{4}, P(B|C) = \frac{3}{6} = \frac{1}{2},$$

$$P(A|C) \cdot P(B|C) = \frac{1}{8}$$

$$P(A \cap B|C) = (\frac{1}{4})(\frac{3}{6}) = \frac{1}{8} = P(A|C) \cdot P(B|C)$$

Yes, it does work.

Theorem 1.12. If two events A and B are conditional independent given an event C with $P(C) > 0$, then:

$$P(A \cap B|C) = P(A|C) \cdot P(B|C)$$

Proof. Recall the general multiplication rule.

$$P(A \cap B) = P(A) \cdot P(B|A)$$

If C happens, then if all the probabilites are adjusted given C, the rule still works.

$$P(A \cap B|C) = P(A|C) \cdot P(B|A, C)$$

Since A, B are conditionally independent given C, $P(B|C) = P(B|A, C)$
Thus,

$$P(A \cap B|C) = P(A|C) \cdot P(B|C)$$

□

Problem 19.1. A bag contains 3 red balls and 2 blue balls. Randomly draw two balls from the bag without replacement. What is the probability of drawing two blue balls?

(Difficulty level: 3)

Solution 19.1a. We can still draw a table to show all possible outcomes. We can label the balls as R_1, R_2, R_3, B_1, B_2 . The sample space of the first trial is $\{R_1, R_2, R_3, B_1, B_2\}$, and the sample space of the second trial depends on what ball is drawn. If R_1 is drawn, then the sample space of the second trial is $\{R_2, R_3, B_1, B_2\}$. There is a total of $5 \cdot 4 = 20$ possible outcomes for two trials.

2nd draw 1st draw	R_1	R_2	R_3	B_1	B_2
R_1	R_1, R_1	R_1, R_2	R_1, R_3	R_1, B_1	R_1, B_2
R_2	R_2, R_1	R_2, R_2	R_2, R_3	R_2, B_1	R_2, B_2
R_3	R_3, R_1	R_3, R_2	R_3, R_3	R_3, B_1	R_3, B_2
B_1	B_1, R_1	B_1, R_2	B_1, R_3	B_1, B_1	B_1, B_2
B_2	B_2, R_1	B_2, R_2	B_2, R_3	B_2, B_1	B_2, B_2

The cells coloured red are impossible outcomes, because we cannot draw the same ball twice from the bag without replacements. So we can ignore these. There are two desired outcomes (shaded in gray), and there are 20 possible outcomes in total, so $P(\text{two balls}) = \frac{2}{20} = \boxed{\frac{1}{10}}$.

Solution 19.1b. Screw all of that outcome listing because it is so time consuming. In the first trial, $P(\text{1st blue}) = \frac{2}{5}$, and in the second trial, there are only one blue ball left (no matter which blue balls you choose), and there are 4 balls left in total, so $P(\text{2nd blue}|\text{1st blue}) = \frac{1}{4}$. So $P(\text{two balls}) = (\frac{2}{5})(\frac{1}{4}) = \boxed{\frac{1}{10}}$.

How about this.

Problem 19.2. A bag contains 3 red balls and 2 blue balls. Randomly draw two balls from the bag without replacement. What is the probability of drawing one red ball and one blue ball?

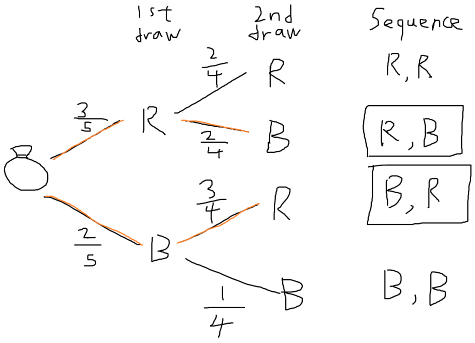
(Difficulty level: 4)

Solution 19.2a. Let's look at the table again.

2nd draw 1st draw	R_1	R_2	R_3	B_1	B_2
R_1	R_1, R_1	R_1, R_2	R_1, R_3	R_1, B_1	R_1, B_2
R_2	R_2, R_1	R_2, R_2	R_2, R_3	R_2, B_1	R_2, B_2
R_3	R_3, R_1	R_3, R_2	R_3, R_3	R_3, B_1	R_3, B_2
B_1	B_1, R_1	B_1, R_2	B_1, R_3	B_1, B_1	B_1, B_2
B_2	B_2, R_1	B_2, R_2	B_2, R_3	B_2, B_1	B_2, B_2

There are 12 desired outcomes and there are 20 possible outcomes in total, so $P(\text{one blue and one red}) = \frac{12}{20} = \boxed{\frac{3}{5}}$.

Solution 19.2b. Instead of a table, we can draw a tree diagram for all the possibilities.



We can multiply probabilities along the branches that leads to the desired sequences, and sum up all of the parallel branches to get the answer.

$P(\text{one blue and one red}) = (\frac{3}{5})(\frac{2}{4}) + (\frac{2}{5})(\frac{3}{4}) = \boxed{\frac{3}{5}}$.

Discussion 19.2b. You may wonder: Why can we multiply the probabilities along the branches? Isn't the two trials dependent? Yes, the trials are dependent, but we have adjusted the probability distribution (with regard to colour of the balls) of the second trial according to the outcome of the first trial. Let's say A is the event of getting a red ball in the first trial, and B is the event of getting a blue ball in the second trial. The two events are dependent, but $P(A \cap B) = P(A) \cdot P(B|A)$ is always true, no matter whether A and B are independent or not. We can see that $P(B|A) = \frac{2}{4}$ in this case.

As for the parallel branches, the two parallel branches lead to the outcomes/ events of the first/second trial that are disjoint (i.e. getting a blue ball and getting a red ball). So we can apply the simple addition rule and sum up the probabilities of all the desired branches.

Lets' practice with more problems.

Problem 20. In a class of 20 students, there are 12 boys and 8 girls. If 4 students are randomly chosen to form a group, what is the probability that the group consists of only boys or only girls (i.e. a single gender only)?

(Difficulty level: 5)

Solution 20. For the first trial, if a boy is chosen, then there are 11 boys remaining and there are 19 students remaining in total. For the second trial (assuming that a boy is chosen in the 1st trial), if a boy is chosen, then there are 10 boys and 18 students remaining respectively. In general, after n trials in which a boy is chosen, there are 12-n boys and 20-n students remaining respectively. Similar arguments can be said for choosing girls.

$P(\text{only boys}) = (\frac{12}{20})(\frac{11}{19})(\frac{10}{18})(\frac{9}{17}) = \frac{33}{323}$
$P(\text{only girls}) = (\frac{8}{20})(\frac{7}{19})(\frac{9}{18})(\frac{5}{17}) = \frac{14}{969}$

Since these two events are mutually exclusive, we can add the probabilities together to get the answer.

$P(\text{only boys}) + P(\text{only girls}) = \frac{33}{323} + \frac{14}{969} = \boxed{\frac{113}{969}}$.

Problem 21. Six dice are each thrown once independently. What is the probability that each number shows up exactly once (Each dice lands on a distinct number)? [3]

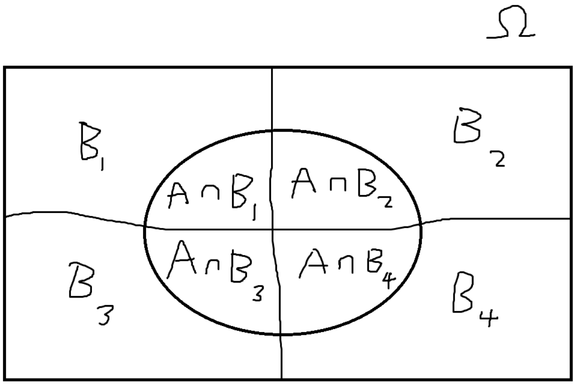
(Difficulty level: 5)

Solution 21. Since the dice throws are independent with identical sample space, we can regard the experiment as a dice thrown six times. For the first trial, any number thrown (from 1 to 6) is desired because there is no previous numbers thrown. So $P(\text{1st distinct})= \frac{6}{6}$. For the second trial, there are 5 desired numbers thrown remaining, since in order to satisfy the requirement, the number thrown cannot be the same as the first trial . There are still 6 possible numbers thrown. In the third, trial, there are 4 desired numbers thrown remaining, and so on. So $P(\text{six distinct numbers}) = (\frac{6}{6})(\frac{5}{6})(\frac{4}{6})(\frac{3}{6})(\frac{2}{6})(\frac{1}{6}) = \boxed{\frac{5}{324}}$.

1.7.2 Law of total probability

The **law of total probability** expresses the idea that the probability of an event $P(A)$ can be partitioned into several products by conditioning A on several events B_i , where B_i are the partitions of the sample space.

To get an intuitive sense of what the law of total probability is about, we can consider a Venn diagram in which the sample space is partitioned into several parts, and event A is sitting in the middle:



In Section 1.6.2, we have obtained a formula

$$A = (A \cap B) \cup (A \cap B')$$

. This is true for any events A, B. Since $A \cap B$ and $A \cap B'$ are disjoint,

$$P(A) = P(A \cap B) + P(A \cap B')$$

, and using the multiplication law for conditional probability $P(A \cap B) = P(A|B) \cdot P(B)$, we can write

$$P(A) = P(A|B) \cdot P(B) + P(A|B') \cdot P(B')$$

This can be extended to any number of disjoint events B_i, such that their union is the entire sample space (/they form a **partition** of the sample space). We have the **law of total probability**.

Theorem 1.13. If there are n events labelled B_1, B_2, ... , B_n such that they form a partition of the sample space , then for any event A we have

$$P(A) = \sum_{i=1}^{n} P(A \cap B_i) = \sum_{i=1}^{n} P(A|B_i)P(B_i) = \sum_{i=1}^{n} P(B_i|A)P(A)$$

Proof. Since B_1, B_2, ... , B_n is a partition of the sample space, we can write

$$\begin{aligned}
\Omega &= \bigcup_{i=1}^{n} B_i \\
A &= A \cap \Omega \\
&= A \cap \left(\bigcup_{i=1}^{n} B_i \right) \\
&= \bigcup_{i=1}^{n} (A \cap B_i) && \text{(by the generalized distributive law)}
\end{aligned}$$

Now note that the sets $A \cap B_i$ are disjoint (since the B_i 's are disjoint). Thus, by the simple addition law (/third probability axiom):

$$P(A) = P(\bigcup_{i=1}^{n} (A \cap B_i)) = \sum_{i=1}^{n} P(A \cap B_i) = \sum_{i=1}^{n} P(A|B_i)P(B_i)$$

□

(Note that the sigma notation $\sum_{i=k}^{n} a_i = a_k + a_{k+1} + \ldots + a_n$.)

Note that if the B_is form a partial partition (the B_i s are disjoint and their union is not the entire sample space /is a proper subset of the sample space), and A is a subset of the union of B_is, we can just let a new term $B_{n+1} = (\bigcup_{i=1}^{n} B_i)'$ so that all the B_is take up the entire sample space. Since $P(A|B_{n+1}) = P(A \cap B_{n+1}) = 0$, $P(A|B_{n+1})P(B_{n+1}) = 0$ and we have:

$$P(A) = \sum_{i=1}^{n} P(A \cap B_i) = \sum_{i=1}^{n} P(A|B_i)P(B_i)$$

The original formula still checks out.

Problem 22. I have three bags that each contain 100 marbles:

- Bag 1 has 75 red and 25 blue marbles;
- Bag 2 has 60 red and 40 blue marbles;
- Bag 3 has 45 red and 55 blue marbles.

I choose one of the bags at random and then pick a marble from the chosen bag, also at random. What is the probability that the chosen marble is red?

(Difficulty level: 4) [1]

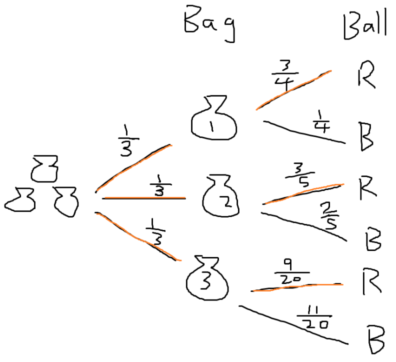
Solution 22a. Let R be the event that the chosen marble is red. Let B_i be the event that I choose Bag i. We already know that

$$P(R|B_1) = \frac{3}{4},$$
$$P(R|B_2) = \frac{3}{5},$$
$$P(R|B_3) = \frac{9}{20}$$

We choose our partition as B_1, B_2, B_3. Note that this is a valid partition because, firstly, the B_is are disjoint (only one of them can happen), and secondly, because their union is the entire sample space as one the bags will be chosen for sure, i.e., $P(B_1 \cup B_2 \cup B_3) = 1$. Using the law of total probability, we can write

$$\begin{aligned} P(R) &= P(R|B_1)P(B1) + P(R|B_2)P(B_2) + P(R|B_3)P(B_3) \\ &= (\frac{3}{4})(\frac{1}{3}) + (\frac{3}{5})(\frac{1}{3}) + (\frac{9}{20})(\frac{1}{3}) \\ &= \boxed{\tfrac{3}{5}}. \end{aligned}$$

Solution 22b. Draw a tree diagram to illustrate the situation.



$P(R) = (\frac{3}{4})(\frac{1}{3}) + (\frac{3}{5})(\frac{1}{3}) + (\frac{9}{20})(\frac{1}{3}) = \boxed{\frac{3}{5}}$.

1.8 Conditional probability

When there are two dependent events, **conditional probability** often arises. Conditional probability focuses on problems like given that A happens, what is the probability that B also happens?

1.8.1 Reduced sample space

For example, in a dice throw, given that the numbers thrown is a prime number, what is the probability that the number is even? In this case, A is getting a prime number, which is $\{2, 3, 5\}$, and B is getting an even number, which is $\{2, 4, 6\}$. If we know that A has already happened, then the possible outcomes are restricted to $A = \{2, 3, 5\}$, so the sample space is reduced to $\{2, 3, 5\}$. Only one of these outcomes is also in B, which is '2'. So the probability $P(B|A) = \frac{1}{3}$.

In general, in an experiment with uniform probability distribution, $P(B|A) = \frac{|A \cap B|}{|A|}$. We also have $P(B|A) = \frac{P(A \cap B)}{P(A)}$, as

$$\begin{aligned} P(B|A) &= \frac{|A \cap B|}{|A|} \\ &= \frac{\frac{|A \cap B|}{\Omega}}{\frac{|A|}{\Omega}} \\ &= \frac{P(A \cap B)}{P(A)} \end{aligned}$$

Note that $P(B|A) = \frac{P(A \cap B)}{P(A)}$ also follows from the fact that $P(A \cap B) = P(A) \cdot P(B|A)$.

By the way, if A and B are disjoint events, then $P(B|A) = 0$, that is if A has already happened, then it is impossible for B to happen since they cannot both happen, and $P(A \cap B) = 0$.

Problem 23. In a class , 60% of the student of them are boys and 35% of the students are boys with glasses. If a student is randomly chosen, what is the probability that the student wears glasses given that he is a boy?

(Difficulty level: 3)

Solution 23a. $P(\text{glasses}|\text{boys}) = \frac{P(\text{boys} \cap \text{glasses})}{P(\text{boys})} = \frac{0.35}{0.6} = \boxed{\frac{7}{12}}$.

Problem 24. I roll a fair dice twice and obtain two numbers X_1= result of the first roll and X_2= result of the second roll. Given that I know $X_1 + X_2 = 7$, what is the probability that $X_1 = 4$ or $X_2 = 4$?

(Difficulty level: 5) [1]

Solution 24. Draw a table to show the possible outcomes.

X_2 X_1	1	2	3	4	5	6
1	1, 1	1, 2	1, 3	1, 4	1, 5	1, 6
2	2, 1	2, 2	2, 3	2, 4	2, 5	2, 6
3	3, 1	3, 2	3, 3	3, 4	3, 5	3, 6
4	4, 1	4, 2	4, 3	4, 4	4, 5	4, 6
5	5, 1	5, 2	5, 3	5, 5	4, 5	5, 6
6	6, 1	6, 2	6, 3	6, 6	4, 5	6, 6

Then calculate the sum.

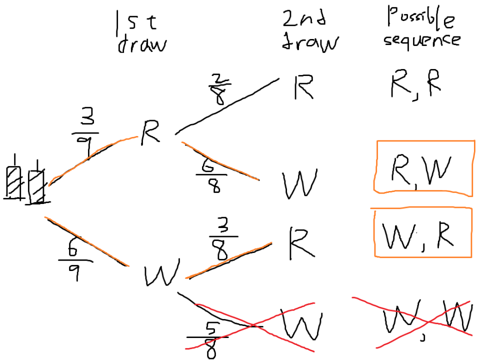
X_2 X_1	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

Since we know that the sum is 7, all of the other sums are impossible. The sample space is reduced to $\{(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)\}$, from which there are two desired outcomes: (3, 4) and (4, 3). So $P(X_1 = 4 \text{ or } X_2 = 4 \mid X_1 + X_2 = 7) = \frac{2}{6} = \boxed{\frac{1}{3}}$.

Problem 25. A box contains 3 red candles and 6 white candles. Two candles are drawn at random from the box without replacement. Given that at least one of the candles drawn is red, what is the probability that exactly one of the candles is red?

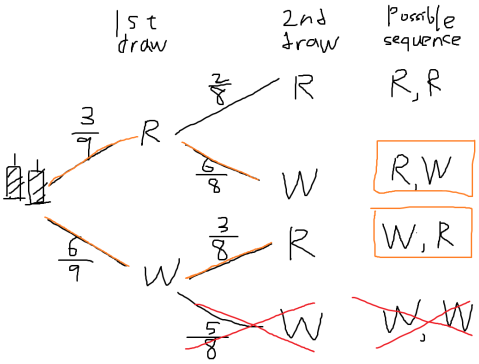
(Difficulty level: 5) [4]

Solution 25. If we were to list out all the possible outcomes, there would be $9 \times 8 = 72$ possible outcomes in total, which is a lot. Instead, we can draw a tree diagram to show the possible sequences. (Note that the possible sequences form a partition of the sample space, and each sequence can be regarded as a single event.)



Since at least one of the candles drawn is red, (W,W) is an impossible sequence. Thus, all of the outcomes in which both candles are white are excluded from the sample space.

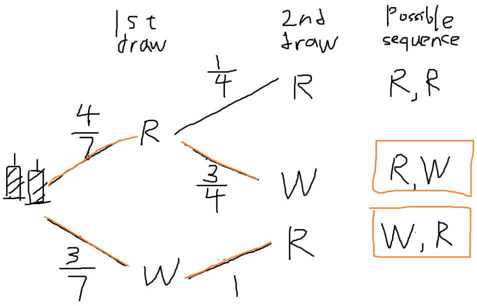
The conditional probability is therefore $\frac{\text{number of desired outcomes}}{\text{number of outcomes in reduced sample space}}$ or $\frac{P(\text{desired outcomes})}{P(\text{outcome in reduced sample space})}$. In this case, the desired outcomes are all the outcomes with exactly one red candles and the reduced sample space is all the outcomes with no white candles.



$$\begin{aligned}
&P(\text{exactly one red candle} \mid \text{at least one red candle})\\
&= \frac{P(\text{exactly one red candle} \cap \text{at least one red candle})}{P(\text{at least one red candle})}\\
&= \frac{P(\text{exactly one red candle})}{1 - P(\text{no red candles})}\\
&= \frac{(\frac{3}{9})(\frac{6}{8}) + (\frac{6}{9})(\frac{3}{8})}{1 - (\frac{6}{9})(\frac{5}{8})}\\
&= \boxed{\frac{6}{7}}
\end{aligned}$$

Discussion 25. You may be like, "Wait a second. Why does all of the probabilities of the possible outcomes in the reduced sample space not sum up to one?" Good question. Yes, in theory, after the condition 'at least one red candle' is known, the probability of the outcomes that satisfy the condition should be updated to sum up to one. But the ratio of the probabilities of different sequences is the same before and after the condition is known, so the probability of each possible sequence is scaled up by a constant factor after knowing the condition, and the numerator and the denominator cancels out.

The tree diagram with updated probability is:



But why is the ratio of the probabilities of different sequences the same before and after the condition is known?

Let RR be the event of getting a red ball and then a red ball in the experiment. Similarly, let RW, WR, WW be the event that the balls drawn are in the sequence (R, W), (W, R), (W, W) respectively. Let A be the event $RR \cup WR \cup WW$ (to shorten the statement).

Since RR is a subset of A, $RR \cap A$=RR. Similarly, $RW \cap A = RW$ and $WR \cap A = WR$.

Recall the conditional probability formula $P(RR|A) = \frac{P(RR\cap A)}{P(A)}$. We also have $P(RW|A) = \frac{P(RW\cap A)}{P(A)}$ and $P(WR|A) = \frac{P(WR\cap A)}{P(A)}$.

Therefore $P(RR|A) = \frac{P(RR)}{P(A)}$, $P(RW|A) = \frac{P(RW)}{P(A)}$, $P(WR|A) = \frac{P(WR)}{P(A)}$.

$$\begin{aligned} P(RR|A) : P(RW|A) : P(WR|A) &= \frac{P(RR)}{P(A)} : \frac{P(RW)}{P(A)} : \frac{P(WR)}{P(A)} \\ &= P(RR) : P(RW) : P(WR) \end{aligned}$$

There is also an assumption to be made: the given condition is obtained by the problem creator without **sampling bias**, and the problem creator will always state the given condition 'honestly'. Imagine that in order to create a conditional probability problem, I need to repeat the whole experiment (1st and 2nd draw are in the same experiment) many many times, say M times (there are M trials of this whole experiment) and randomly sample one trial of the experiment that satisfy the condition.

Every time A happens, the problem will say "given that at least one candles drawn is red", and if WW happens, the problem will never say that, and will say "given that none of the candles drawn are red" instead. So in roughly $(P(RR) + P(RW) + P(WR)) \cdot M$ times, the problem will say "given that at least one candles drawn is red". Otherwise, say, if the problem states the condition only when RR happens, and omits the condition when RW and RW happen, then the sample is biased. If we know that a problem is sampled this way, then RR has a 100% chance of happening, which also means RW or WR have 0% chance of happening. So in every conditional probability problem, the given condition is always assumed to be obtained in a way without sampling bias.

As the ratio of the probabilities of different sequences the same before and after the condition is known, the proportion of the number of times that RR, RW and WR occur in these $(P(RR)+P(RW)+P(WR))\cdot M$ trials is roughly $P(RR) : P(RW) : P(WR)$.

If I randomly, with uniform probability, draw a sample experiment from the $(P(RR) + P(RW) + P(WR)) \cdot M$ trials that RR or RW or WR has happened, the sampling of the problem will be unbiased.

This is because in a uniform probability distribution, if the number of desired outcomes of some events B_1, B_2, B_3 are $|B_1|$, $|B_2|$, $|B_3|$ respectively, and there are N possible outcomes, then
$P(B_1) = \frac{|B_1|}{N}$, $P(B_2) = \frac{|B_2|}{N}$, $P(B_3) = \frac{|B_3|}{N}$.

$P(B_1) : P(B_2) : P(B_3) = \frac{|B_1|}{N} : \frac{|B_2|}{N} : \frac{|B_3|}{N} = |B_1| : |B_2| : |B_3|$

Conditional probability can be confusing sometimes. Let's try the 'Boy or girl paradox'.

Problem 26.1. Mr. Jones has two children. The older child is a girl. What is the probability that both children are girls? (Assume that the genders of the children are independent and the probabilities of each gender is equal.)

(Difficulty level: 3) [5]

Solution 26.1. (Copied from [6]) Listing the gender of older child first, our sample space is $\{$BB, BG, GB, GG$\}$. The event "the older child is a girl" is $\{$GB, GG$\}$ and the event "both children are girls" is $\{$GG$\}$. Thus the probability that both children are girls given the older child is a girl is $\boxed{\frac{1}{2}}$.

Problem 26.2. Mr. Smith has two children. At least one of them is a boy. What is the probability that both children are boys? (Same assumption as above)

(Difficulty level: 4) [5]

Solution 26.2. (Copied from [6]) The event "at least one child is a boy" is $\{$BB, BG, GB$\}$ so the probability that both children are boys is $\boxed{\frac{1}{3}}$.

1.8.2 Bayes' theorem

Suppose that we know $P(A|B)$, but we are interested in the probability $(B|A)$. This is where **Bayes' theorem** comes in. Using the multiplication rule for conditional probability:

$$P(A|B)P(B) = P(A \cap B) = P(B|A)P(A)$$

$$P(A|B)P(B) = P(B|A)P(A)$$

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)}$$

Similarly,

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

Theorem 1.14. The Bayes' theorem states that

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)}$$

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

By the law of total probability, $P(A) = \sum_{i=1}^{n} P(A|B_i)P(B_i)$. Thus, the Bayes' theorem can be expanded as follows:

Theorem 1.15. If $B_1, B_2, \ldots, B_n$ form a partition of the sample space, then for any A,

$$P(B_j|A) = \frac{P(A|B_j)P(B_j)}{\sum_{i=1}^{n} P(A|B_i)P(B_i)}$$

If the partition is B and its complement B' (which means $n = 2$), then the formula can be expressed as:

$$P(B|A) = \frac{P(A|B)P(B)}{P(A|B)P(B) + P(A|B')P(B')}$$

Problem 27. A certain disease affects about 1 out of 10,000 people. There is a test to check whether the person has the disease. The test is quite accurate. In particular, we know that

- the probability that the test result is positive (suggesting the person has the disease), given that the person does not have the disease, is only 2 percent;
- the probability that the test result is negative (suggesting the person does not have the disease), given that the person has the disease, is only 1 percent.

A random person gets tested for the disease and the result comes back positive. What is the probability that the person has the disease? (Express the answer in decimal form.)

(Difficulty level: 5) [1]

Solution 27a. Let D be the event that the person has the disease, and let T be the event that the test result is positive. We know

$$P(D) = \frac{1}{10000},$$

$$P(T|D') = 0.02,$$

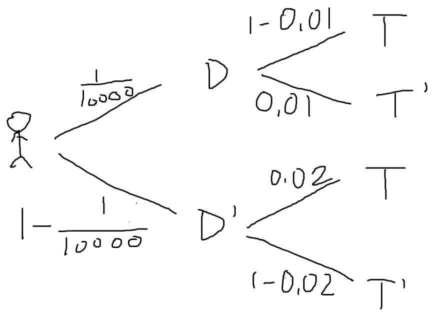
$$P(T'|D) = 0.01,$$

What we want to compute is $P(D|T)$. Using Bayes' theorem:

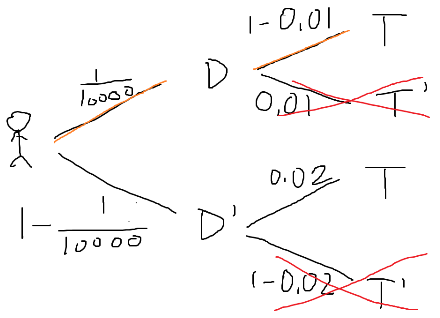
$$\begin{aligned}
P(D|T) &= \frac{P(T|D)P(D)}{P(T|D)P(D)+P(T|D')P(D')} \\
&= \frac{(1{-}0.01)\times 0.0001}{(1{-}0.01)\times 0.0001+0.02\times(1{-}0.0001)} \\
&= \boxed{\tfrac{1}{203}}
\end{aligned}$$

This means that there is less than half a percent chance that the person has the disease.

Solution 27b. Draw a tree diagram.



Given the condition that the test result is positive, eliminate impossible outcomes to show the reduced sample space and the desired outcome.



$$\begin{aligned}
P(D|T) &= \frac{P(T|D)P(D)}{P(T|D)P(D)+P(T|D')P(D')} \\
&= \frac{(1{-}0.01)\times 0.0001}{(1{-}0.01)\times 0.0001+0.02\times(1{-}0.0001)} \\
&= \boxed{\tfrac{1}{203}}
\end{aligned}$$

2 Combinatorics

Sometimes, the sample space for multiple experiments or trials get big pretty quick. We cannot draw a table and count the desired outcomes one by one. It is also not convenient to use a tree diagram as there would be too many branches. That's why we need to learn some counting methods. The study of how we count things is called **combinatorics**.

If there are several experiments or trials, each with uniform probability distribution, then each combination of outcomes in the experiments/trials is equally likely to happen. Thus, the formula $P(A) = \frac{\text{Number of desired outcomes}}{\text{Total number of possible outcomes}}$ holds. The number of desired outcome is also the number of ways that A can happen. If we know how to find the number ways A can happen, then we can find the probability of A.

2.0 Preface

2.0.1 Multiplication principle

Recall the **multiplication principle**. If there are k things to do, and there are n_1 ways to do the first thing, n_2 ways to do the second thing, $\ldots$, and n_k ways to do the kth thing, then the total number of ways to do the k things is $n_1 n_2 \ldots n_k$.

For example, if I have 4 T-shirts labelled T_1, T_2, T_3, T_4, and 3 (pairs of) shorts labelled S_1, S_2, S_3, then the set of outfits I can wear is
$\{(T_1, S_1), (T_1, S_2), (T_1, S_3), (T_2, S_1), (T_2, S_2), (T_2, S_3),$
$(T_3, S_1), (T_3, S_2), (T_3, S_3), (T_4, S_1), (T_4, S_2), (T_4, S_3)\}$.

For each of the T-shirts, I can pair it with 3 choices of shorts. There are 4 T-shirts in total. So the total number of outfits is $3+3+3+3 = 4 \times 3 = 12$. (Assuming I cannot go naked.)

Now, let's say I become nearsighted, and need to wear glasses. I have 2 glasses in total, labelled G_1, G_2. So for each of the 12 original outfits, I can wear G_1 or G_2. There are a total of $12 \times 2 = 24$ new outfits in total. You get the idea.

Because of the commutative property of multiplication (which means the order in which we multiply numbers does not change the product), any order we do the k things does not change the total number of ways to do the thing. I can do the k th thing first and the 1st thing last. In the above example, any order I wear the clothes and glasses does not change the total number of outfits available. That means that we can arbitrarily label the things from 1 to k.

2.0.2 Four common types of sampling

When we randomly draw an element from a sample space with uniform probability, it is called **sampling**. The element drawn is called a sample.

Sampling can be done with or without replacement. If it is done **with replacement**, the sample space remains unchanged after the sampling, so for multiple samplings, repetition of the sample drawn is allowed. For example, if I throw a dice two times, both dice throws can land on ‘6’, so the sampling of each dice throw is done with replacement.

If sampling is done **without replacement**, then the element drawn is removed from the sample space after each individual sampling, so for multiple samplings, repetition of the sample drawn is not allowed. For example, from a bag of distinctly labelled balls, when I draw a ball labelled ‘1’ without replacement, I cannot draw ball ‘1’ from the bag again. The sequence (ball ‘1’ , ball ‘1’) is not allowed.

Sampling can also be done with or without order. In three dice throws, if we consider the sequence (‘1’, ‘2’, ‘3’) a different thing from (’3’, ’2’, ’1’), then sampling is **ordered** (/order matters).

If we consider the (‘1’, ‘2’, ‘3’) the same thing as (’3’, ’2’, ’1’), then sampling is **unordered** (/order doesn’t matter). Note that for unordered sampling, (‘1’, ‘1’, ‘3’) and (‘1’, ‘3’, ‘3’) are considered different things.

Thus, we have four types of sampling:

1. ordered sampling with replacement

2. ordered sampling without replacement

3. unordered sampling without replacement

4. unordered sampling with replacement

Each type of sampling has a different formula and must be treated differently.

Type 2 (ordered sampling without replacement) is called **permutations**. Type 3 (unordered sampling without replacement) is called **combinations**. Type 1 is called Cartesian product and type 4 is called ‘stars and bars’ (relating to how we count type 4 sampling).

2.1 Ordered sampling with replacement

This is the simplest case. Common examples of ordered sampling with replacement are coin flips, dice throws and password strings. It is often ordered sampling with replacement when there are multiple independent experiments or trials.

Recall the multiplication principle. Now set $n_1 = n_2 = \ldots = n$. If there are k things to do, and there are n ways to do each thing, then the total number of ways to do the k things is n^k .

For example, if there are k dice throws, then the total number of possible sequences of numbers thrown is 6^k, as there are 6 numbers to choose from for the first throw, and 6 numbers to choose from for the second throw, and so on. We can think of it as choosing k samples from the sample space {1, 2, 3, 4, 5, 6} with replacement with order.

Theorem 2.1. If repetition is allowed and order matters, the total number of ways to choose k objects from a set with n elements is n^k .

Problem 28. Suppose that the password of a website must consist of 4 upper case letters. If Bob chooses each upper case letter at random to make his password, what is the probability that the password is 'SEAT' or 'EATS'?

(Difficulty: 4)

Solution 28a. There are a total of 26^4 possible passwords, each with equal probability, and there are two desired passwords.

$$P(\text{'SEAT' or 'EATS'}) = \frac{2}{26^4} = \boxed{\frac{1}{228488}}$$

Solution 28b. Let A be the event of choosing 'S' or 'E' as the first letter. $P(A) = \frac{2}{26}$. If 'S' is chosen, the next letter must be 'E'. If 'E' is chosen as the first letter instead, the next letter must be 'A'. In either case, the probability that the second letter is the desired letter is $\frac{1}{26}$. The third and fourth letter also has $\frac{1}{26}$ probability each to be the desired letter.

$$P(\text{'SEAT' or 'EATS'}) = (\frac{2}{26})(\frac{1}{26})(\frac{1}{26})(\frac{1}{26}) = \boxed{\frac{1}{228488}}$$

There are a total of 26^4 possible passwords, each with equal probability, and there are two desired passwords.

Discussion 28b. Viewing each time of choosing letters as independent events is sometimes more complicated than just counting the desired outcomes and total number of outcomes, so we will often use the latter method in combinatorics.

2.2 Ordered sampling without replacement: Permutations

This case commonly arises when we are drawing balls from a bag without replacement, choosing distinct elements from a set or arranging stuff. Ordered sampling without replacement are often dependent experiments or trials.

For example, if there are two dice throws, the number of ways that the two numbers thrown are distinct is 6×5 . (This is discussed in Problem 19.) It is because for the 1st throw, there are 6 choices for the number thrown. For the 2nd throw, there are only 5 choices left for distinct number thrown. If there are k dice throws, then for the kth throw, there are only $6 - (k - 1)$ choices left for distinct numbers thrown. (For $k > 6$, there are no choices for distinct number thrown so the number of ways becomes 0 .) The number of ways of throwing k distinct numbers is therefore $6 \times 5 \times \ldots \times (6 - k + 1)$. We write this as P^6_k.

In general, if repetition is not allowed and order matters, the total number of ways to choose k object from a set with n elements is P^n_k , where $P^n_k = n \times (n-1) \times \ldots \times (n-k+1)$. If $k > n$, then $P^n_k = 0$. The permutation of the k objects chosen is called a k-permutation of the set.

Another example is arranging numbers. If I want to arrange the numbers 1, 2, 3, then for the 1st position, there are 3 choices of numbers. For the 2nd position, there are 2 choices of numbers left. For the 3rd (last) position, there are only 1 number left. All the arrangements are { (1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1) }. There are a total of $3 \times 2 \times 1 = 6$ arrangements/permutations of the numbers.

In general, the number of ways to arrange k distinct objects is

$$k \times (k - 1) \times \ldots \times 2 \times 1$$

. We denote this number by $k!$, where '!' is the **factorial** of k. So for any positive integer k,

$k! = k \times (k-1) \times \ldots \times 2 \times 1$. We also define $0! = 1$ so that $\frac{(k+1)!}{k!} = k$ for all non-negative integers. Note that $P^n_n = n!$. So we can regard the number of ways to arrange/permute n distinct objects as the number of ways to choose n distinct objects from a set n elements where order matters.

So we have

$$\begin{aligned} P_k^n &= n \times (n-1) \times \ldots \times (n-k+1) \\ &= \frac{n \times (n-1) \times \ldots \times 1}{(n-k) \times (n-k-1) \times \ldots \times 1} \\ &= \frac{n!}{(n-k)!} \end{aligned}$$

Theorem 2.2. If repetition is not allowed and order matters, the total number of ways to choose k objects from a set with n elements is $P_k^n = \frac{n!}{(n-k)!}$, for $0 \leq k \leq n$.

Stated more concisely, the number of k-permutations of an n-element set is P_k^n.

Problem 29.1. Adrian, Billy, Catherine and 4 other students are arranged randomly in a row. What is the probability that Adrian, Billy and Catherine all stand next to each other?

(Difficulty level: 6) [4]

Discussion 29.1. When some objects or people are arranged randomly in a row, it means that each arrangement/permutation is equally likely to appear. How the shuffling is done or what algorithm is used does not matter.

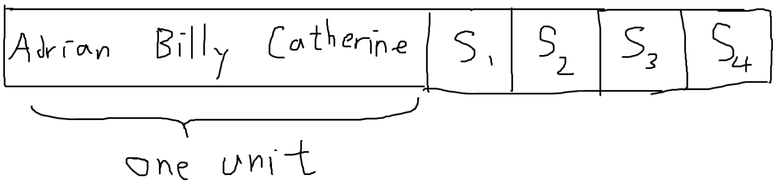
It could be that initially, the 7 students are unordered. One student is randomly chosen to be at the 1st position. Then one of the remaining students is randomly chosen to be at the 2nd position, and so on.

Or it could be that Adrian randomly chooses a position to occupy. Then Billy randomly chooses one of the remaining positions to occupy, and so on.

Or the students could label themselves from 1 to 7, then randomly choose a permutation from a list of the 7! permutations of 7 distinct numbers to arrange themselves.

These methods all result in a uniform probability distribution where each permutation is equally likely to appear.

Solution 29.1. Since Adrian, Billy and Catherine must stand next to each other, we can treat them as one unit. For example,



Number of ways of arranging the 4 other students and 1 unit
$= (4 + 1)! = 5!$

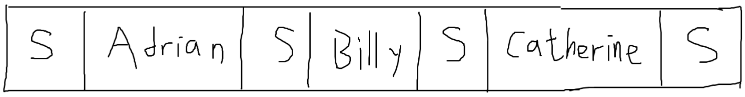
Number of ways of arranging Adrian, Billy and Catherine (within the unit) $= 3!$

P(stand next to each other)$= \frac{5!\times 3!}{7!} = \boxed{\frac{1}{7}}$.

Problem 29.2. Adrian, Billy, Catherine and 4 other students are arranged randomly in a row. What is the probability that Adrian, Billy and Catherine stand alternately with the other students (Adrian, Billy and Catherine are sandwiched between the other 4 students, such that each of them is separated by one other student)?

(Difficulty level: 6) [4]

Solution 29.2. Since Adrian, Billy and Catherine must be separated by a student, they must stand in an arrangement like this (where Adrian, Billy, Catherine can switch places):



Number of ways of arranging the 4 other students
$= 4!$

Number of ways of arranging Adrian, Billy and Catherine $= 3!$

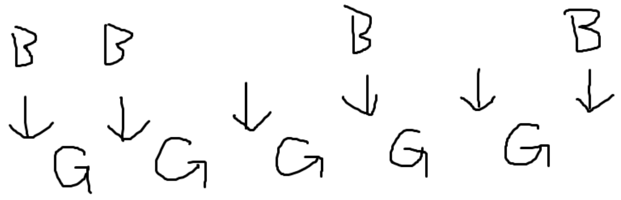
P(stand alternately)$= \frac{3!\times 4!}{7!} = \boxed{\frac{1}{35}}$

Problem 30. If 4 boys and 5 girls randomly forms a queue, what is the probability that no boys are next to each other in the queue?

(Difficulty level: 7) (2016 DSE Maths P1 Q15)

Solution 30a. If a boy is at the front or end of the queue. Then he must stand next to one girl. If a boy is at the middle of the queue, then he must be standing between two girls. Also note that there can only be a maximum of one boy between two girls, but there can be one or two girls between two boys.

The space between the girls (and the front/end of queue) create some 'slots' for boys to stand in. We can draw a diagram to illustrate this.

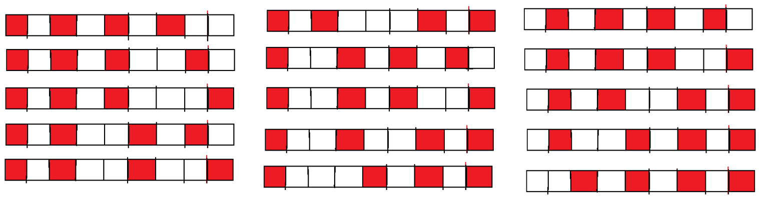


There are 6 slots in total, and each of the 4 boys can occupy a distinct slot, The total number of ways to do this with regard to order is P_4^6.

The number of arrangements within the girls is 5!. So we have

$$P(\text{no boys next}) = \frac{P_4^6 \times 5!}{9!} = \boxed{\frac{5}{42}}$$

Solution 30a. We can count the number of ways no boys stand next next to each other without regard to the order within the same gender. (Each red block represents a boy and each white block represents a girl.)



There are a total of 15 ways this can be done. The number of permutations within the boys is 4! and the number of permutations within the girls is 5!.

$$P(\text{no boys next}) = \frac{15 \times 4! \times 5!}{9!} = \boxed{\frac{5}{42}}$$

Problem 31. If k people are at a party, what is the least number of k such that the probability that at least two of them have the same birthday is more that 50% ?

(Assume that the birthdays of any two person are independent , and there are 365 days in a year, and all days are equally likely to be the birthday of a specific person.)

(Difficulty level: 7) [1]

Solution 31. Let A be the event that at least two people have the same birthday. The phrase "at least" suggests that it might be easier to find the probability of the complement event, $P(A')$. This is the event that no two people have the same birthday, and we have

$$P(A) = 1 - \frac{|A'|}{|\Omega|}$$

where Ω is the sample space, the set of all possible sequence of birthdays of k people. (We can arbitrarily label the people from 1 to k, then put person 1 birthday at the 1st position of the sequence, and person 2 at the 2nd position of the sequence, and so on.) There are 365 choices for the first person, 365 choices for the second person, ... 365 choices for the kth person, so there are 365^k possible sequences of birthdays in total, so $|\Omega| = 365^k$.

Now let's find $|A'|$. If no birthdays are the same, this is similar to finding $|\Omega|$ with the difference that repetition is not allowed, so we have

$$|A'| = P_n^k = n\times(n-1)\times\ldots\times(n-k+1)$$

You can see this directly by noting that there are $n = 365$ choices for the first person, $n-1 = 364$ choices for the second person, ... , $n-k+1$ choices for the kth person. Thus the probability of A can be found as

$$\begin{aligned} P(A) = 1 - \frac{P_k^{365}}{365^k} &> \frac{1}{2} \\ \frac{P_k^{365}}{365^k} &< \frac{1}{2} \\ \frac{365!}{(365-k)!\cdot(365^k)} &< \frac{1}{2} \end{aligned}$$

By guessing and checking with a calculator, we get $k = 23$.

2.3 Unordered sampling without replacement

This case commonly arises when we want to find the number of ways that k heads show up in n coin flips, choosing k identical objects (but not the same element) from a set of n elements, or colour k squares in a row of n squares.

2.3.1 Combinations

Suppose there is a bag with 7 balls labelled from '1' to '7'. We want to draw three balls from the bag without replacement and put them in a row. The 1st ball drawn is put to the left, 2nd to the middle, and 3rd to the right. There are P_3^7 ways this can be done. Consider all the cases in which '1', '2', '3' are drawn from the bag. There are $3! = 6$ cases because the three balls can be arranged in 3! ways. These are the cases that the combination of balls is '1', '2', '3' (For combinations, the order of '1', '2', '3' is not important to us.). Therefore, in 3! of the P_3^7 ways, the balls drawn are considered the same combination (a single case of combination) of '1', '2', '3'. A different combination can be '1', '6', '7' or '2', '3', '4' , but '1', '6', '7' and '1', '7', '6' are the same combination.

There are P_3^7 3-permutations of the 7 balls in the bag, and every 3! of them is considered a single combination. So the total number of 3-combinations of the 7 balls is $\frac{P_3^7}{3!}$. We denote this number by C_3^7 . In general,

Theorem 2.3. If repetition is not allowed and order does not matter, the total number of ways to choose k objects from a set with n elements is

$$C_k^n = \frac{P_k^n}{k!} = \frac{n!}{k! \cdot (n-k)!} \text{ , for } 0 \leq k \leq n$$

.

Stated more concisely, the number of k-combinations of an n-element set is C_k^n. C_k^n is also called a **binomial coefficient**.

Note that $\dfrac{C_k^a}{C_k^b} = \dfrac{P_k^a}{P_k^b}$ for any $a, b \geq k$.

Also note that $C_k^n = C_{n-k}^n$, and $C_0^n = C_n^n = 1$.

Also, $C_1^n = C_{n-1}^n = n$ and $C_2^n = C_{n-2}^n = \frac{n(n-1)}{2}$.

Also, if $n < k$, then C_k^n is defined to be 0 , no matter whether n is positive or not.

Problem 32. 3 blue balls and 5 red balls are randomly arranged in a row. What is the probability that the first 3 balls in the row are all blue balls?

(Difficulty level: 6)

Solution 32a. Number of ways of arranging 8 balls = 8!

Number of ways of putting 3 blue balls in the first three positions with order = 3!

Number of ways of putting 5 red balls in the last five positions with order = 5!

P('BBBRRRRR')= $\dfrac{3! \times 5!}{8!} = \boxed{\dfrac{1}{56}}$

Solution 32b. We regard the blue balls as identical to other blue balls and red balls are identical to other red balls. (But a blue ball and red ball are distinct to each other.) So if only the 3 blue balls are put in a row, there is only one way to arrange them (B, B, B) . In general, when the order of some objects is not important to us, we can regard it as there is only one way to arrange the objects.

Number of ways of putting 3 blue balls in the first three positions without order = 1

Number of ways of putting 5 red balls in the last five positions without order = 1

Number of ways of arranging 3 identical blue balls and 5 identical red balls in the same row = C^8_3

P('BBBRRRRR')= $\dfrac{1}{C^8_3} = \boxed{\dfrac{1}{56}}$

Discussion 32b. But why is the number of ways of arranging 3 identical blue balls and 5 identical red balls in the same row = C^8_3 ?

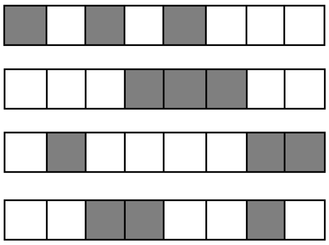
We can label the positions of the row from '1' to '7' because each position is distinct. i.e. $(B, \_) \neq (\_, B)$. The case that the three blue balls are in the first three positions can be expressed as the combination of '1', '2', '3'. So the total number of combinations of the positions of 3 blue balls is just the total number of combinations of 3 distinct integers from 1 to 8 , which is C^8_3. We don't need to consider red balls because there is only one way to put them into the remaining 5 positions. (Note that we can also only consider the positions of red balls and neglect blue balls since $C^8_3 = C^8_5$. It is a matter of perspective.)

Each of the C^8_3 combination of positions of blue balls has an equal chance of appearing because every 3! × 5! of the 8! permutations is a single case of the combination. As probability of permutations is uniformly distributed,

$$P(\text{’1’,‘2’,‘3’}) = P(\text{’1’,‘6’,‘7’ or whatever}) = \frac{3! \times 5!}{8!}$$

Similar to arranging balls in a row, when there is a row of n uncoloured (or white) blocks, the total number of ways to colour k blocks with a single colour (say gray) is C_k^n .

Some ways to colour 3 blocks in a row of 8 blocks:



We can see that the blocks are divided into two parts: gray and uncoloured, and there are a total of C_3^8 ways to divide the blocks by colouring 3 of the 8 blocks.

Therefore, the total number of ways to divide n distinct objects into two groups A and B where group A consists of k objects and group B consists of $n - k$ (without regard to the order of objects within the same group) is also C_k^n.

2.3.2 Arranging identical and distinct objects

As you can see in Solution 29b, we can regard some objects as **identical** or **distinct**, depending on whether we care about the order of the chosen objects. For distinct objects a, b, the arrangement (a, b) is not the same as (b, a), but for identical objects a, b, (a, b) is the same arrangement as (b, a). Note that when two objects are identical, it does not mean that they are the same, and they still account for two elements belonging to the same set.

For example, if there are two unlabelled identical blue balls a, b put into a row, we cannot tell the two arrangements (a, b) or (b, a) apart, so we will regard them as identical. However, the set of the blue balls $\{a, b\}$ has two elements. Now, if I write the label ‘a’, ‘b’ on each ball, then when I put the balls on a row, I can tell each of them apart.

For another example, suppose I have some cards that each consist of an letter in the alphabet. If I have five cards ‘E’, ‘A’, ‘R’, ‘T’, ‘H’, then I can arrange them in 5! ways since each card is distinct. If the cards I have are

'S', 'T', 'E', 'V', 'E' instead, then how many ways can I arrange them? Let's first label the 'E's as 'E_1' and 'E_2' so we can tell them apart. The number of arrangements is still 5!. However, if I now remove the label, then for two particular arrangements ('S', 'T', 'E_1', 'V', 'E_2') and ('S', 'T', 'E_2', 'V', 'E_1') have both become the same arrangement ('S', 'T', 'E', 'V', 'E'). The same can be said for all other arrangements. So there are only $\frac{5!}{2!}$ unique ways to arrange 'S', 'T', 'E', 'V', 'E'.

Now what if the cards I have is 'T', 'E', 'E', 'T', 'H'? Then for four (2!×2!) particular labelled arrangements
('T_1', 'E_1', 'E_2', 'T_2', 'H'),
('T_1', 'E_2', 'E_1', 'T_2', 'H'),
('T_2', 'E_1', 'E_2', 'T_1', 'H'),
('T_2', 'E_2', 'E_1', 'T_1', 'H')
, they have all become the same unlabelled arrangement ('T', 'E', 'E', 'T', 'H'). So there are only $\frac{5!}{2 \times 2!}$ unique ways to arrange the letters. In general,

Theorem 2.4. When there are m types of identical objects, namely object A_1 , object $A_2, \ldots$, object A_m, and there are a total of k_1 identical object A_1, k_2 identical object $A_2, \ldots$, k_m identical object A_m, the total number of unique ways to arrange the $n = k_1 + k_2 + \ldots + k_m$ objects is

$$\frac{n!}{k_1! \times k_2! \times \ldots \times k_m!}$$

Note that if $m = 2$ (there are two types of identical objects), the formula becomes $C^n_{k_1} = \frac{n!}{k_1!(n-k_1)!}$. This is just like the case in Problem 29, or colouring a row of blocks.

If $m = 3$, it becomes $C^n_{k_1} C^{n-k_1}_{k_2} = \frac{n!}{k_1!(n-k_1)!} \frac{(n-k_1)!}{k_2!(n-k_1-k_2)!} = \frac{n!}{k_1!k_2!k_3!}$

In general, we can see that

$$\frac{n!}{k_1! \times k_2! \times \ldots \times k_m!} = C^n_{k_1} C^{n-k_1}_{k_2} C^{n-k_1-k_2}_{k_3} \ldots C^{k_{m-1}+k_m}_{k_{m-1}} C^{k_m}_{k_m}$$

This number is also called a **multinomial coefficient**.

Note that the number of ways to divide n distinct objects into m distinct groups (without regard to order of objects in the same group), each with size k_i, is also given by this formula. (Seems like there is some sort of duality between the two situations.)

Problem 33. A bag contains a red ball, a green ball and a blue ball. I randomly draw a ball from the bag, record its colour, and put it back into the bag. This whole procedure is then repeated 9 more times (so 10 times in total). What is the probability of drawing the red ball exactly 3 times, the blue ball exactly 5 times, and the green ball exactly 2 times?

(Difficulty level: 7)

Solution 33. This is a 'sampling with replacement' problem, but we can use the concept of combinations/permutations to help us. Label the balls 'R' (red), 'G' (green), 'B' (blue) respectively. A possible sequence of draws can be 'RRBGGGGRBR' or whatever. Note that the 'R's are identical because there is only one way to draw only the red balls in the sequence (R, R, R, ...). We cannot draw the 2nd red ball in the 1st trial or 1st red ball in the 2nd trial. The same can be said for 'B's and 'G's. So the total number of sequences with 3R, 5B, 2G is $\dfrac{10!}{3! \times 5! \times 2!}$.

The total number of possible sequences is 3^{10}.

$$\begin{aligned} P(3R, 5B, 2G) &= \frac{\frac{10!}{3! \times 5! \times 2!}}{3^{10}} \\ &= \boxed{\frac{280}{6561}} \end{aligned}$$

Problem 34. A dice is thrown 18 times. What is the probability that each number appears exactly 3 times?

(Difficulty level: 7) [1]

Solution 34. How many distinct (unique) sequences are there with three 1's, three 2's, ..., and three 6's? Each sequence has 18 positions which we need to fill with the digits. To obtain a sequence, we need to choose three positions for 1's, three positions for 2's, ..., and three positions for 6's. The number of ways to do this is given by the multinomial coefficient

$$\frac{18!}{3! \cdot 3! \cdot 3! \cdot 3! \cdot 3! \cdot 3!}$$

The total number of possible sequences is 6^{18}.

Thus the required probability is:

$$\begin{aligned}&P(\text{each number appear 3 times})\\ =\ &\frac{\frac{18!}{3!\cdot 3!\cdot 3!\cdot 3!\cdot 3!\cdot 3!}}{6^{18}}\\ =\ &\boxed{\frac{14889875}{11019960576}}\end{aligned}$$

Problem 35. I have 8 identical balls, a red bag, a green bag and a blue bag. I randomly choose a bag and put a ball inside the chosen bag. This is then repeated 7 times (so 8 times in total). What is the probability each bag contains at least 2 balls?

(Difficulty level: 7)

Solution 35. Let (r, g, b) denote case in which the number of balls in red bag is r, green bag is g and blue bag is b . There are six desired permutations of number of balls in each bag, which are (4, 2, 2), (2, 4, 2), (2, 2, 4), (3, 3, 2), (2, 3, 3), (3, 2, 3).

For the combination (4, 2, 2), there are $\frac{8!}{4!\times 2!\times 2!}$ ways to put the balls inside the bag. Same can be said for (2, 4, 2) and (2, 2, 4).

For the combination (3, 3, 2), there are $\frac{8!}{3!\times 3!\times 2!}$ ways to put the balls inside the bag. Same can be said for (2, 3, 3) and (3, 2, 3).

There are a total of 3^8 possible ways to put the balls inside the bag.

$$\begin{aligned}P(\text{at least 2 balls each bag}) &= \frac{\frac{8!}{4!\times 2!\times 2!}\times 3+\frac{8!}{3!\times 3!\times 2!}\times 3}{3^8}\\ &= \frac{2940}{6561}\\ &= \boxed{\frac{980}{2187}}\end{aligned}$$

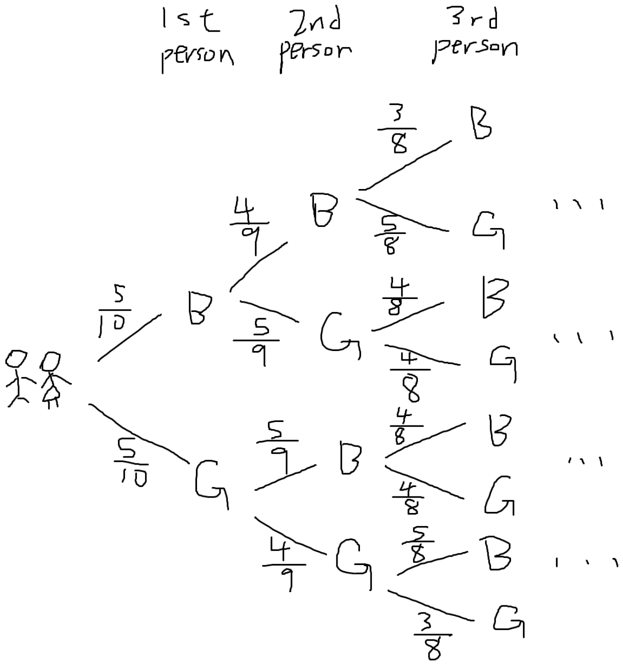
2.3.3 Combinations of two or more types of objects

Now, what if we draw something without replacement, so that repetition is not allowed anymore, and we only care about the number of something drawn?

Problem 36. A working group of 5 is selected at random from a committee of 5 girls and and 5 boys. What is the probability that the group includes 2 girls and 3 boys?

(Difficulty level: 6) [4]

Solution 36a. Draw a partial tree diagram.



No matter what path that leads to the desired outcomes in the tree diagram is chosen, the path must pass through exactly 2 girls and 3 boys. Otherwise, it is not a desired outcome anymore. The probability that a specific path that leads to a desired outcome is chosen is $(\frac{5}{10})(\frac{4}{9})(\frac{3}{8})(\frac{4}{7})(\frac{3}{6}) = \frac{5}{126}$

The number of ways of arranging BBBGG in a row (B & B identical, G & G identical) is $C^5_2 = 10$

P(2 girls and 3 boys)$= 10 \cdot (\frac{5}{126}) = \boxed{\frac{25}{63}}$

Discussion 36a. When we are walking along a specific path in the tree diagram, we have already taken the order within the same gender of people into account, but we haven't taken the order between the two genders into account, so to compensate, we multiply the number of ways to arrange BBBGG with identical BB's and GG's.

Solution 36b. Since the order of the people selected is not important to us,

Number of ways of selecting 2 girls from 5 girls $= C_2^5$

Number of ways of selecting 3 boys from 5 boys $= C_3^5$

Number of ways of forming a group including 2 girls and 3 boys $= C_2^5 \times C_3^5$

$$P(\text{2 girls and 3 boys}) = \frac{C_2^5 \times C_3^5}{C_5^{10}} = \boxed{\frac{25}{63}}$$

Discussion 36b. Why does this work? First, we can distinctly label the boys B_1 , B_2 , B_3 , B_4 , B_5 and girls G_1 , G_2 , G_3 , G_4 , G_5 . Each 5-combination of the 10 people has an equal chance of occurring, and there is a total of C_5^{10} 5-combinations.

(B_1, B_2, B_3, B_4, G_3) and (G_3, B_4, B_3, B_2, B_1,) is the same combination, but (B_2, B_3, B_5, G_2, G_4) and (B_1, B_4, B_5, G_2, G_4) are different combinations. We need to find the number of combinations that consist of exactly 3 boys and 2 girls. We can split it into two cases: the number of 3-combinations of the 5 boys and the number of 2-combinations of the 5 girls.

Number of 3-combinations of the 5 boys $= C_3^5$

Number of 2-combinations of the 5 girls $= C_2^5$

For each of the C_3^5 combinations of boys, we can pair it with C_2^5 choices of combinations of girls, so there are a total of $C_3^5 \times C_2^5$ ways to make a group of 5 people with 3 boys and 2 girls.

Then we just use the formula $P(A) = \frac{\text{Number of desired outcomes}}{\text{Number of possible outcomes}}$ and we are done.

This method of calculating probability can be generalized to any situations when there are two types of objects to choose from, and we don't care about the order they are selected.

Theorem 2.5. When there are two types of objects to choose from, namely object A and object B, and there are a total of a object A's and b object B's, if a total of $k = k_1 + k_2$ objects are randomly chosen without replacement, the probability of choosing exactly k_1 object A's and k_2 object B's is:

$$\frac{C_{k_1}^a \times C_{k_2}^b}{C_{k_1+k_2}^{a+b}}$$

This can be further generalized to n types objects to choose from.

When there are n types of objects to choose from, namely object A_1 , object A_2, …, object A_n, and there are a total of a_1 object A_1, a_2 object A_2, … , a_n object A_n, if a total of $k = k_1 + k_2 + \ldots + k_n$ objects are randomly chosen, the probability of choosing exactly k_1 object A_1, k_2 object A_2, … , k_n object A_n without regard to order is

$$\frac{C^{a_1}_{k_1} \times C^{a_2}_{k_2} \times \ldots \times C^{a_n}_{k_n}}{C^{a_1+a_2+\ldots+a_n}_{k_1+k_2+\ldots+k_n}}$$

Hypergeometric distribution

When we only care about how many of a particular type of object, say object A's, are chosen, the probability distribution of choosing exactly k object A's follows the **hypergeometric distribution**. The formula for hypergeometric distribution is a variant of the formula in Theorem 2.5. In this case, drawing an object A is regarded as a success and drawing a type of object other than object A is regarded as a failure.

Theorem 2.5b. When there are N objects to choose from, and the N objects contain a successes and $N-a$ failures, if n objects are randomly chosen without replacement, then the probability of choosing exactly k succeses is:

$$P(k) = \frac{C^a_k \times C^{N-a}_{n-k}}{C^N_n}$$

Problem 37. In a box, there are 3 blue plates, 7 green plates and 9 purple plates. If 4 plates are randomly selected from the box at the same time, what is the probability that at least 2 plates of different colours are selected?

(Difficulty level: 6) (2020 DSE Maths P1 Q15(b))

Discussion 37. Selecting some objects 'at the same time' means selecting them without replacement and we don't care about the order the objects are selected. We can still arbitrarily label the objects A_1, A_2, … , A_n but (A_1, A_2, A_3) and (A_3, A_1, A_2) are the same thing to us. Each combination of objects has an equal chance to be selected.

Solution 37. It is easier to find the probability that all the plates are of the same colour first, then use the complement rule to get the answer.

Number of ways of selecting 4 plates of the same colour $= 0 + C_4^7 + C_4^9$

Number of ways of selecting 4 plates from 19 plates $= C_4^{19}$

$$\begin{aligned} P(\text{at least 2 different plates}) &= 1 - \frac{C_4^7 + C_4^9}{C_4^{19}} \\ &= \boxed{\frac{3715}{3876}} \end{aligned}$$

Problem 38. In a bag, there are 4 green pens, 7 blue pens and 8 black pens. If 5 pens are randomly drawn from the box at the same time, what is the probability that not more than 2 green pens are drawn?

(Difficulty level: 7) (2017 DSE Maths P1 Q17(c))

Discussion 38. We can regard blue pens and black pens as the same type of pens, like 'unwanted pens'. So there are 4 green pens and 15 unwanted pens in total.

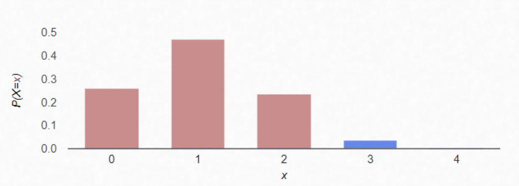
Solution 38. We can find the probability of getting exactly 3 pens and probability of getting exactly 4 pens first.

$$P(\text{3 green pens}) = \frac{C_3^4 \times C_2^{15}}{C_5^{19}} = \frac{35}{969}$$

$$P(\text{4 green pens}) = \frac{C_4^4 \times C_1^{15}}{C_5^{19}} = \frac{5}{3876}$$

$$\begin{aligned} &P(\text{not more than 2 green pens}) \\ &= 1 - P(\text{3 green pens}) - P(\text{4 green pens}) \\ &= 1 - \frac{35}{969} - \frac{5}{3876} \\ &= \boxed{\frac{3731}{3876}} \end{aligned}$$

For reference, the bar graph of the probability distribution of the number of green pens drawn is:



Problem 39. 5 students from a group of 20 students are chosen randomly to join a singing contest. Mary, Emily and John are three students in the group. What is the probabilities that Mary and Emily are chosen but not John?

(Difficulty level: 6)

Solution 39. To find the number of desired outcomes for picking and not picking some specific elements in a set, we can employ the 'lock and block' method. Since John is not chosen, we 'block' him and there are 19 students remaining, from which we pick 5 of them. Since Mary and Emily are chosen, we 'lock' them, and there are 17 students remaining, from which we freely pick 3 of them.

The total number of possible outcomes is C_5^{20}.

$$P(\text{Mary and Emily but not John}) = \frac{C_3^{17}}{C_5^{20}} = \boxed{\frac{5}{114}}$$

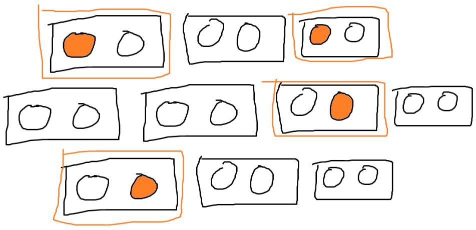
Discussion 39. In general, when we 'block' an element, we reduce the number of elements to choose from by 1, but the number of picks available remains unchanged , and when we 'lock' an element, we reduce both the number of elements to choose from and the number of picks by 1.

What if there are many types of objects/people, and we don't necessarily need to choosing a particular type of objects/people?

Problem 40. There are 10 clubs in a school. 2 students are nominated from each club to join a leadership training camp. From the nomination list, 4 students are chosen at random. What is the probability that the 4 students chosen are all from different clubs?

(Difficulty level: 6)

Solution 40. We can visualize the situation with a diagram. The rectangles represent clubs and the circles represent students in the nomination list.



Total number of ways of choosing 4 students from the list $= C_4^{20}$

First, we consider the total number of ways to choose 4 clubs from 10 clubs, which is C_4^{10}.

Then we consider the total number of ways of choosing 1 student from each of the 4 chosen clubs, which is 2^4.

$$P(\text{all from different clubs}) = \frac{C_4^{10} \times 2^4}{C_4^{20}} = \boxed{\frac{224}{323}}$$

Problem 41.1. In a box, there are 3 green balls, 4 red balls, 5 blue balls and a black ball. Amy and Ben play a game. They take turn to draw 2 balls randomly from the box at the same time. The player who first draws a black ball wins the game and the game ends. If the player does not draw a black ball, the 2 balls drawn will be put back to the box. Amy draws the ball first.

What is the probability that Ben wins the game in 3 draws or less by him?

(Difficulty level: 7) (Maths Mock P1 Q16(a))

Solution 41. A trial consists of drawing 2 balls at the same time (so balls drawn without replacement within the same trial), and for multiple trials, the balls are drawn with replacements after each trial. In each trial (drawing 2 balls), if a black ball is drawn, then the other ball drawn is one of the 12 non-black balls, so there are 12 ways to draw a black ball (without order) in a trial. The probability of drawing a black ball is $\frac{12}{C_2^{13}} = \frac{2}{13}$.

There are 3 desired events: Ben wins in his 1st turn, Ben wins in his 2nd turn, Ben wins in his 3rd turn.

Let A denotes Amy's turn and B denotes Ben's turn. For the desired events (Ben wins in his 3 turns or less), the game must follow the sequence 'AB', 'ABAB', 'ABABAB' . To explain it in detail:

If Amy draws the black ball first, then she wins and it is not possible for Ben to win. So she must draw a non-black ball in her 1st turn. This has a probability of $\frac{11}{13}$.

After Amy draws a non-black ball, it is now Ben's 1st turn. If Ben draws a black ball in his 1st turn, then he wins. Overall, this has a probability of $(\frac{11}{13})(\frac{2}{13})$, and is one of the desired events.

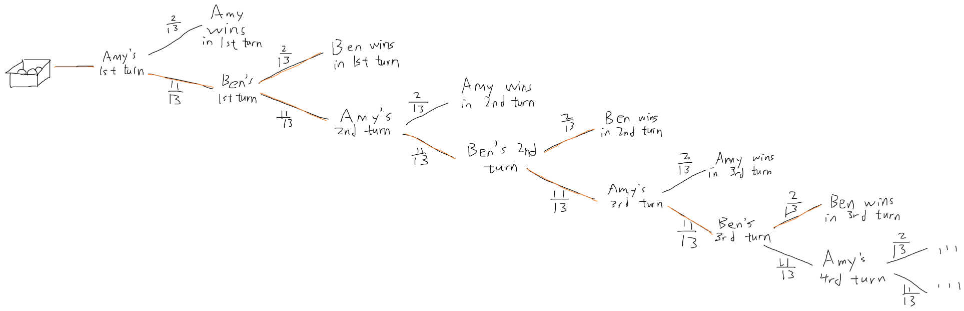
Otherwise, Ben draws a black ball in his first turn with an overall probability of $(\frac{11}{13})(\frac{11}{13})$. Now it is back to Amy's 2nd turn. In Amy's 2nd turn, she must also draw a non-black ball in order for Ben to have his 2nd turn. The overall of Amy drawing a non-black ball in her 2nd turn is $(\frac{11}{13})(\frac{11}{13})(\frac{11}{13})$.

Ben draws a black ball in his 2nd turn with an overall probability of $(\frac{11}{13})(\frac{11}{13})(\frac{11}{13})(\frac{2}{13}) = (\frac{11}{13})^3(\frac{2}{13})$.

With the same reasoning, Ben draws a black ball in his 3rd turn with an overall probability of $(\frac{11}{13})^5(\frac{2}{13})$.

$$\begin{aligned}
&P(\text{Ben wins in his 3 draws or less})\\
&= \left(\frac{11}{13}\right)\left(\frac{2}{13}\right) + \left(\frac{11}{13}\right)^3\left(\frac{2}{13}\right) + \left(\frac{11}{13}\right)^5\left(\frac{2}{13}\right)\\
&= \boxed{\frac{1400322}{4826809}}
\end{aligned}$$

For reference, the tree diagram of the game is:



Problem 41.2. (The base situation is the same as Problem 36.1.)

The player who wins the game can draw one extra ball immediately. The player will get \$50, \$40, or \$30 if the extra ball drawn is green, red or blue respectively. What is the probability that Ben wins the game in his first draw and gets \$30 ?

(Difficulty level: 6)

Solution 41.2. If (given that) Amy doesn't win in her 1st turn, the probability that Ben draws a blue ball and a black ball in his 1st turn is $\frac{5}{C_2^{13}}$. If (given) that happens, he wins the game, and there are 4 blue balls left and a total of 11 balls left. Without putting back the blue and black balls drawn, he will draw another blue ball with a probability of $\frac{4}{11}$.

If (again, given that) Amy doesn't win her 1st turn, the probability that Ben draws a non-blue ball and a black ball in his 1st turn is $\frac{7}{C_2^{13}}$. If (given) that happens, he wins the game, and there are 5 blue balls left and a total of 11 balls left. Without putting back the non-blue and black balls drawn, he will draw another blue ball with a probability of $\frac{5}{11}$.

Therefore, the overall probability of Ben winning in his first draw and then drawing a blue ball, thus getting \$30 is

$$(\frac{11}{13})(\frac{5}{C_2^{13}})(\frac{4}{11}) + (\frac{11}{13})(\frac{7}{C_2^{13}})(\frac{5}{11}) = \boxed{\frac{55}{1014}}$$

Now what if we want to find the probability that a player wins the game in any number of turns?

Problem 42.1. Ada and Billy play a game consisting of two rounds. In the first round, Ada and Billy take turns to throw a fair dice. The player who first gets a number '3' wins the first round. Ada and Billy play the first round until one of them wins. Ada throws the dice first.

What is the probability that Ada wins the first round of the game?

(Difficulty level: 6) (2014 DSE Maths P1 Q19(a))

Solution 42.1a. ('Two rounds' is irrelevant when considering only this subproblem. We can regard it as only one round/game.) The number of turns it takes to win the game for any player can range from 1 to infinity, because theoretically, the game can go on and on forever without any players getting a '3' in a dice throw, if they are both unlucky.

Let A_i be the event that Ada wins in her i th turn.

$P(A_1) = \frac{1}{6}$

$P(A_2) = (\frac{5}{6})^2(\frac{1}{6})$

$P(A_3) = (\frac{5}{6})^4(\frac{1}{6})$
$P(A_4) = (\frac{5}{6})^6(\frac{1}{6})$
$P(A_n) = (\frac{5}{6})^{2n-2}(\frac{1}{6})$

$$\begin{aligned} P(\text{Ada wins}) &= P(A_1) + P(A_2) + P(A_3) + \dots \\ &= \frac{1}{6} + \left(\frac{5}{6}\right)^2\left(\frac{1}{6}\right) + \left(\frac{5}{6}\right)^4\left(\frac{1}{6}\right) + \dots \end{aligned}$$

We can see that it is an (infinite) **geometric series** [9] . The first term a is $\frac{1}{6}$ and the common ratio r is $(\frac{5}{6})^2$. We can use the formula for geometric series:

$$S = \frac{a}{1-r}\ , \text{ for } |r| < 1$$

to get

$$P(\text{Ada wins}) = \frac{\frac{1}{6}}{1-(\frac{5}{6})^2} = \boxed{\frac{6}{11}}$$

Discussion 42.1a. The geometric series formula can be derived as follows:

Let S be the geometric series $a + ar + ar^2 + ar^3 + \dots$, where $|r| < 1$. We have

$$\begin{aligned} rS &= ar + ar^2 + ar^3 + ar^4 + \dots \\ rS &= S - a \\ a &= S(1-r) \\ S &= \frac{a}{1-r} \end{aligned}$$

Solution 42.1b. Let p be the probability that the first person who throws the dice win the first round of the game.

If Ada does not get '3' in her 1st turn, Billy will have his 1st turn. That has a $\frac{5}{6}$ chance of happening. Now we can pretend that Billy is the first person to throw the dice in the round. So Billy has p overall probability of throwing a '3' in his 1st turn or 2nd turn or [any number] th turn.

[9] Geometric series is the sum of an infinite number of terms that have a constant ratio between successive terms. In general, a geometric series is written as $a+ar+ar^2+ar^3+...$

Going back to the original situation where Ada throws the dice first, Billy will have $\frac{5p}{6}$ probability of winning the round. Also notice that the probability that either Ada or Billy win the round is 1. So we have:

$$\begin{aligned} p + \frac{5p}{6} &= 1 \\ \frac{11p}{6} &= 1 \\ p &= \boxed{\frac{6}{11}} \end{aligned}$$

Problem 42.2. (The base situation is same as above.)

In the second round of the game, two balls are dropped one by one into a device containing eight tubes arranged side by side (see Figure 8). When a ball is dropped into the device, it falls randomly into one of the tubes. Each tube can hold more than 1 balls.

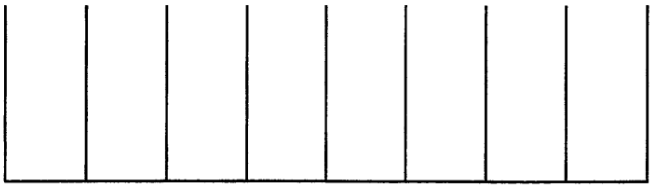


Figure 8

Only the winner of the first round plays the second round. If the two balls fall into the same tube or two adjacent tubes, then the player gets 10 tokens. Otherwise, the player gets no tokens.

What is the probability that Ada gets no tokens in the whole game (consisting of 1st and 2nd rounds)?

(Difficulty level: 6) (2014 DSE Maths P1 Q19(biii) Modified)

Solution 42.2. Note that if Ada doesn't win the first round, she will also get no tokens.

In the 2nd round,

Number of ways that two balls fall into the same tube = 8

Number of ways that two balls fall into two adjacent tubes = $7 \times 2!$

Total number of ways that two balls fall into the tubes = 8^2

Overall,

$$\begin{aligned} & P(\text{Ada gets 10 tokens in the game}) \\ = & \left(\frac{6}{11}\right)\left(\frac{8+7\times 2!}{8^2}\right) \\ = & \frac{3}{16} \end{aligned}$$

$$P(\text{Ada gets no tokens}) = 1 - \frac{3}{16} = \boxed{\frac{13}{16}}$$

Now let's try some poker hand problems.

Problem 43. Alex and Bob are each given a 52-card poker deck (so there are two decks in total). They each randomly draw 5 cards from their own deck without replacement. Here are some possible combinations of the 5 cards (called a poker hand) drawn by each person:

Two-pair: Two cards have one rank, two cards have another rank, and the remaining card has a third rank. e.g. {♡2, ♤2, ♡5, ♧5, ♢K}

Three-of-a-kind: Three cards have one rank and the remaining two cards have two other ranks. e.g. {♡2, ♤2, ♧2, ♧5, ♢K}

What is the probability that Alex draws a two-pair and Bob draws a three-of-a-kind?

(Difficulty level: 7) ([7] Modified)

Discussion 43. Recall that a poker deck consists of 52 cards, which is a Cartesian product of the 4 suits {♢, ♧, ♡, ♤} and the 13 ranks {2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K}.

Solution 43. (Copied from [8]) To count the number of desired outcomes for each person's hand, we create each hand by a sequence of actions and use multiplication principle to count how many ways it can be done. (Critically, the number of choices available at each step is independent of the choices made in the earlier steps.)

Two-pairs:

We first choose two of thirteen ranks for the two pairs. C^{13}_2

For the pair of lower rank, we choose two of four suits. C^4_2

For the pair of higher rank, we choose two of four suits. C^4_2

For the singleton card, we choose one of eleven remaining ranks: C^{11}_1

For the singleton card, we choose one of four suits. C_1^4 .

$P(\text{Alex draws a two-pair}) = \dfrac{C_2^{13}(C_2^4)^2 C_1^{11} C_1^4}{C_5^{52}} = \dfrac{198}{4165}$

Three-of-a-kind:

We choose one of thirteen ranks for the triple. C_1^{13}

We choose three of four suits for the triple. C_3^4

For the other two cards, we choose two of twelve remaining ranks. C_2^{12}

For the singleton of higher rank, we choose one of four suits: C_1^4

For the singleton of lower rank, we choose one of four suits: C_1^4

$P(\text{Bob draws a three-of-a-kind}) = \dfrac{C_1^{13} C_3^4 C_2^{12} (C_1^4)^2}{C_5^{52}} = \dfrac{88}{4165}$

$P(\text{both happening}) = (\dfrac{198}{4165})(\dfrac{88}{4165}) = \boxed{\dfrac{17\,424}{17\,347\,225}}$

You can calculate the probability of other poker hands using a similar strategy. The full list is here:

`http://en.wikipedia.org/wiki/Poker_probability`

2.3.4 Binomial distribution

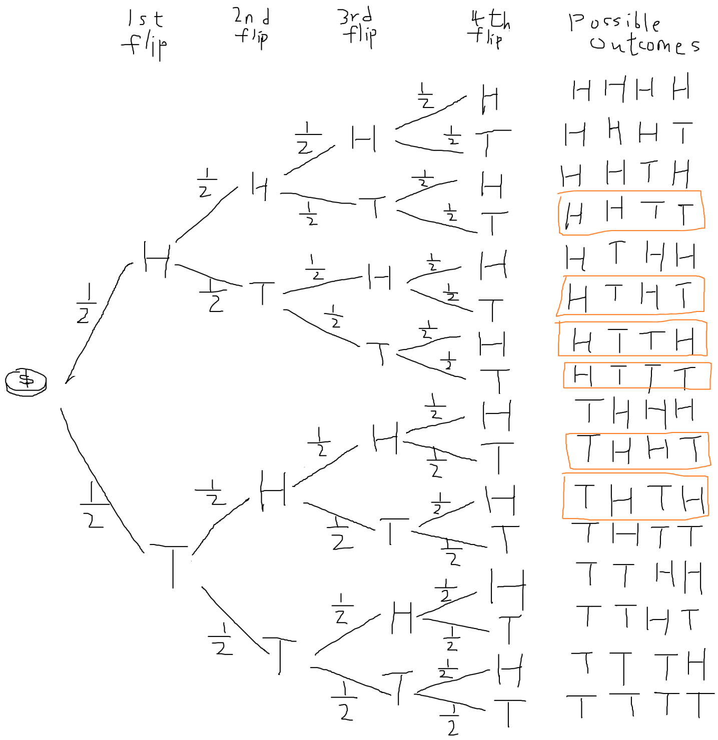
The formula for combinations is actually useful for situations in which there are independent trials that allows repetition of samples drawn.

If a fair coin is flipped n times, what is the probability of getting exactly k heads? This also involves the number of ways to choose k objects from a set of n elements.

Problem 44.1. A fair coin is flipped 4 times. What is the probability of getting exactly 2 heads and 2 tails?

(Difficulty level: 4)

Solution 44.1a. We can draw a tree diagram:



Number of desired outcomes $= 6$

Number of possible outcomes $= 2^4 = 16$

$P(2 \text{ heads, } 2 \text{ tails}) = \frac{6}{16} = \boxed{\frac{3}{8}}$

Solution 44.1b. Note that the number of ways of getting exactly 2 heads and 2 tails is the number of ways to arrange HHTT in a row. There are $C_2^4 = 6$ ways to do that. Since each arrangement is equally likely,

$$P(2 \text{ heads, } 2 \text{ tails}) = \frac{C_2^4}{2^4} = \frac{6}{16} = \boxed{\frac{3}{8}}$$

Problem 44.2. A fair coin is flipped 4 times. What is the probability of getting at least 2 heads?

(Difficulty level: 5)

Solution 44.2.

$$\begin{aligned}P(\text{at least 2 heads}) &= P(\text{2 heads}) + P(\text{3 heads}) + P(\text{4 heads})\\ &= \frac{C_2^4}{2^4} + \frac{C_3^4}{2^4} + \frac{C_4^4}{2^4}\\ &= \frac{6}{16} + \frac{4}{16} + \frac{1}{16}\\ &= \boxed{\tfrac{11}{16}}\end{aligned}$$

We can see that in general, the probability of getting exactly k heads and $n-k$ tails in n coin flips is

$$\frac{C_k^n}{2^n}$$

We can see that all of the probabilities of the possibilities sum up to one since

$$P(\text{any number of heads}) = \sum_{k=0}^{n} \frac{C_k^n}{2^n} = \frac{1}{2^n}\sum_{k=0}^{n} C_k^n = \frac{1}{2^n}(2^n) = 1$$

Note that $\sum_{k=0}^{n} C_k^n = 2^n$ because of the **binomial theorem**, which states that for any non-negative integer n and real number x, y,

$$(x+y)^n = \sum_{k=0}^{n} C_k^n x^{n-k} y^k$$

Putting $x = y = 1$, we have

$$\begin{aligned}(1+1)^n &= \sum_{k=0}^{n} C_k^n (1^{n-k})(1^k)\\ 2^n &= \sum_{k=0}^{n} C_k^n\end{aligned}$$

Since we are here already, I will provide a proof for the binomial theorem using mathematical induction.

Proof of binomial theorem

First, we prove the Pascal's identity $C_k^n + C_{k-1}^n = C_k^{n+1}$.

$$\begin{aligned}
C_k^n + C_{k-1}^n &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\
&= n!\left[\frac{1}{k!(n-k)!} + \frac{1}{(k-1)!(n-k+1)!}\right] \\
&= n!\left[\frac{n-k+1}{k!(n-k+1)!} + \frac{k}{k!(n-k+1)!}\right] \\
&= n!\left[\frac{n+1}{k!(n-k+1)!}\right] \\
&= \frac{(n+1)!}{k!(n+1-k)!} \\
&= C_k^{n+1}
\end{aligned}$$

We have the statement $(x+y)^n = \sum_{k=0}^{n} C_k^n x^{n-k} y^k$.
.When $n=0$, LHS $= (x+y)^0 = 1$, RHS $= \sum_{k=0}^{0} C_k^0 x^{0-k} y^k = 1$.
$\therefore$ The statement is true for $n=0$.

When $n=1$, LHS $= x+y$,
RHS $= \sum_{k=0}^{1} C_k^1 x^{1-k} y^k = C_0^1 x^{1-0} y^0 + C_1^1 x^{1-1} y^1 = x+y$.
$\therefore$ The statement is true for $n=1$.

Assume that for some non-negative integer m,

$$(x+y)^m = \sum_{k=0}^{m} C_k^m x^{m-k} y^k$$

When $n = m + 1$,

$$\begin{aligned}
\text{LHS} &= (x+y)^{m+1} \\
&= (x+y)\sum_{k=0}^{m} C_k^m x^{m-k} y^k \qquad \text{(Inductive hypothesis)} \\
&= x\sum_{k=0}^{m} C_k^m x^{m-k} y^k + y\sum_{k=0}^{m} C_k^m x^{m-k} y^k \\
&= \sum_{k=0}^{m} C_k^m x^{m-k+1} y^k + \sum_{k=0}^{m} C_k^m x^{m-k} y^{k+1}
\end{aligned}$$

Putting the index $j = k + 1$ for the summation in the right,

$$= \sum_{k=0}^{m} C_k^m x^{m-k+1} y^k + \sum_{j=1}^{m+1} C_{j-1}^m x^{m-(j-1)} y^j$$

Extracting the first term and last term of the two summations respectively

$$\begin{aligned}
&= \left(C_0^m x^{m-0+1} y^0 + \sum_{k=1}^{m} C_k^m x^{m-k+1} y^k \right) \\
&\quad + \left(\sum_{j=1}^{m} C_{j-1}^m x^{m-(j-1)} y^j + C_m^m x^{m-(m+1-1)} y^{m+1} \right) \\
&= x^{m+1} + y^{m+1} + \sum_{k=1}^{m} C_k^m x^{m-k+1} y^k + \sum_{j=1}^{m} C_{j-1}^m x^{m-j+1} y^j
\end{aligned}$$

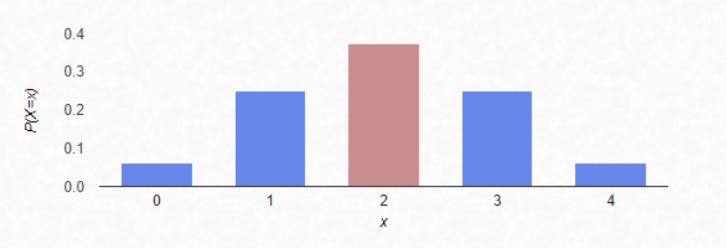
Since the index j is just a dummy variable, we can put back $k = j$,

$$\begin{aligned}
&= x^{m+1} + y^{m+1} + \sum_{k=1}^{m} C_k^m x^{m-k+1} y^k + \sum_{k=1}^{m} C_{k-1}^m x^{m-k+1} y^k \\
&= x^{m+1} + y^{m+1} + \sum_{k=1}^{m} \left(C_k^m + C_{k-1}^m \right) x^{m-k+1} y^k \\
&= x^{m+1} + y^{m+1} + \sum_{k=1}^{m} C_k^{m+1} x^{m-k+1} y^k \qquad \text{(Pascal's identity)} \\
&= C_0^{m+1} x^{m+1-0} y^0 + C_{m+1}^{m+1} x^0 y^{m+1} + \sum_{k=1}^{m} C_k^{m+1} x^{m+1-k} y^k \\
&= \sum_{k=0}^{m+1} C_k^{m+1} x^{m+1-k} y^k \\
&= \text{RHS}
\end{aligned}$$

By mathematical induction, $(x+y)^n = \sum_{k=0}^{n} C_k^n x^{n-k} y^k$ is true for all non-negative integers n. □

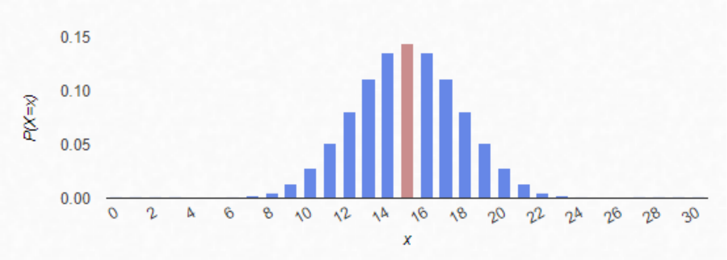
Bar graph of binomial distribution

The probability distribution of the total number of heads that show up in n coin flips follows the **binomial distribution**. If there are 4 coin flips, and X is the number of heads that show up, the bar graph of the probability distribution of X is: (By the way, X is called a **random variable**, and x is the possible values that X can take on.)



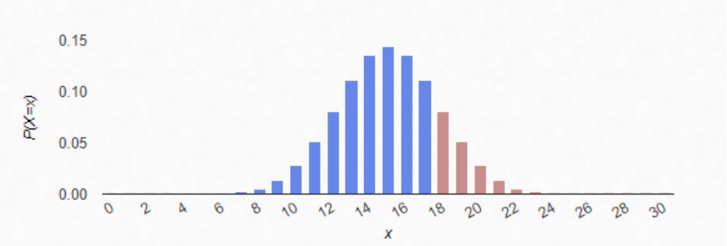
We can see that 2 heads and 2 tails is the mostly likely outcome. The bar graph is symmetric because heads and tails are equally likely to show up. Also, we know that $C_k^n = C_{n-k}^n$. So if X is the number of tails that show up, it will still follow the same distribution.

If there are 30 coin flips instead:



15 heads and 15 tails is the mostly likely outcome. This makes sense, as the probability of heads and probability of tails is $\frac{1}{2}$ each. Notice that the probability of getting less than 6 tails or more than 24 tails is so small that it can't even be seen in the graph.

If we want to find the probability that at least k heads show up, we can sum up the probabilities of each $x \geq k$.



If $k = 18$, then I can find the probability

$$P(X \geq 18) = \sum_{i=18}^{30} \frac{C_i^{30}}{2^{30}} \approx 0.1808$$

Alternatively, we can first find $P(X \geq 16)$ by finding $\frac{1-P(X=15)}{2}$ because the two sides of the distribution is symmetric.

So $P(X \geq 16) = \dfrac{1 - \frac{C_{15}^{30}}{2^{30}}}{2} \approx 0.4278$

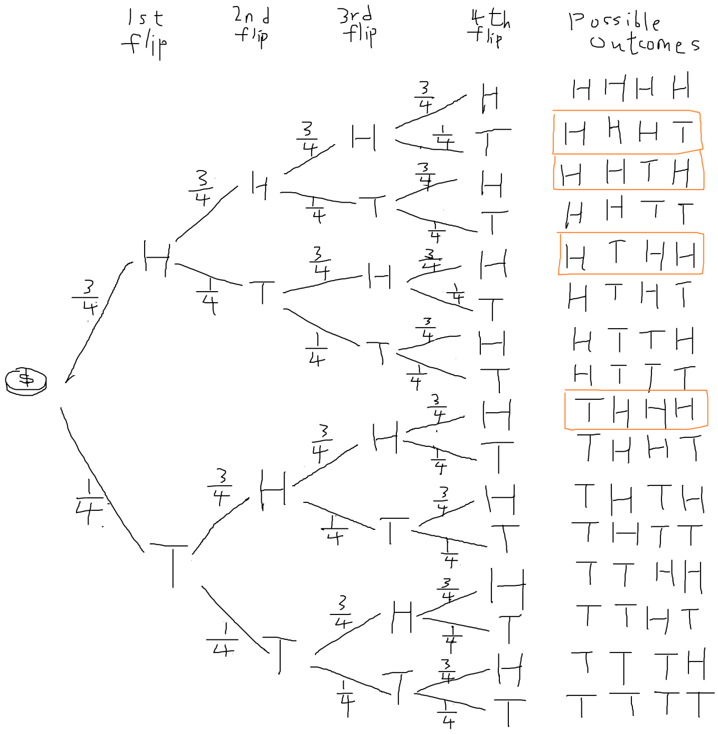
$$\begin{aligned} P(X \geq 18) &= 0.4278 - P(X = 16) - P(X = 17) \\ &= 0.4278 - \frac{C_{16}^{30}}{2^{30}} - \frac{C_{17}^{30}}{2^{30}} \\ &\approx 0.1808 \end{aligned}$$

Now what if I have a biased coin instead?

Problem 45. A biased coin has $\frac{3}{4}$ probability of landing on heads and $\frac{1}{4}$ probability of landing on tails. When the coin is flipped 4 times, what is the probability of getting exactly 3 heads and 1 tail?

(Difficulty level: 5)

Solution 45a. Draw a tree diagram.

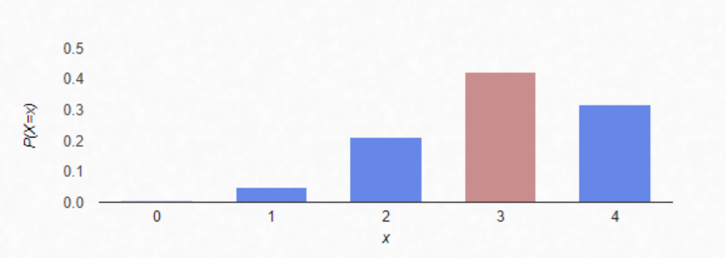


$$\begin{aligned}P(3 \text{ heads, } 1 \text{ tail}) &= (\frac{3}{4})(\frac{3}{4})(\frac{3}{4})(\frac{1}{4}) + (\frac{3}{4})(\frac{3}{4})(\frac{1}{4})(\frac{3}{4}) + (\frac{3}{4})(\frac{1}{4})(\frac{3}{4})(\frac{3}{4}) \\ &\quad + (\frac{1}{4})(\frac{3}{4})(\frac{3}{4})(\frac{3}{4}) \\ &= (\frac{3}{4})(\frac{3}{4})(\frac{3}{4})(\frac{1}{4}) \times 4 \\ &= \boxed{\frac{27}{64}}\end{aligned}$$

Solution 45b. We can see that in the tree diagram, there are C^4_3 ways to go to the desired outcomes, because there are C^4_3 ways to arrange HHHT in a row.

So $P(3 \text{ heads, } 1 \text{ tail}) = C^4_3 \left(\frac{3}{4}\right)^3 \left(\frac{1}{4}\right) \times 4 = \boxed{\frac{27}{64}}$

Discussion 45b. The probability distribution of the number of heads in 4 biased coin flips is:



The distribution is not symmetric anymore. This makes sense, as it should be more likely to get 4 heads instead of 0 heads.

This method to calculate the probability not only works for coin flips, but also any other experiments or trials that has only two outcomes. A trial with only two possible outcomes is called **Bernoulli trial**, and these outcomes are called '**success** ' (S) and 'failure ' (F), depending on what our desired outcomes are. Multiple Bernoulli trials in an experiment are independent, which means the probability of success is the same every time the experiment is conducted.

A coin flip, biased or not, is an example of Bernoulli trial. If we want to find the total number of heads that occur in n coin flips, then we can regard 'heads' in each flip as a success, and 'tails' as a failure. If we want to find the number of tails instead, then we can regard 'tails' as success and 'heads' as failure.

If we want to find the number of '6's that occur in n dice throws, we can regard getting a '6' as a success and getting any other numbers as a failure. Thus, by defining our desired outcomes, we can transform any experiments or trials into a Bernoulli trial.

The probability of getting k successes in n Bernoulli trials can be calculated using the method in Solution 30b. We have the formula for binomial distribution:

Theorem 2.6. If in a Bernoulli trial, the probability of success is p and the probability of failure is $1-p$, then the probability of getting k successes in n Bernoulli trials is

$$P(k) = C_k^n \cdot p^k \cdot (1-p)^{n-k}$$

The formula basically says that we multiply the probability of success k times since there are k successes, and multiply the probability of failure $n-k$ times since there are $n-k$ failures, then multiply the number of ways of getting exactly k successes and $n-k$ failures.

Note that the probabilities of all possibilities (from 0 success to n successes) sum up to 1. This makes sense, as by the binomial theorem (first let $q = 1-p$),

$$P(\text{any number of successes}) = \sum_{k=0}^{n} C_k^n \cdot p^k \cdot q^{n-k} = (p+q)^n$$

As $p+q=1$, the sum of probabilities is also 1.

We can observe that each term of the binomial expansion resembles the probability of a particular number of successes. This is because distributing probabilities according to the number of successes in n trials is just doing a binomial expansion of $(p+q)^n$, and each Bernoulli trial increases the power n by one.

Problem 46. What is the probability of getting exactly three '6' in seven dice throws?

(Difficulty level: 6)

Solution 46. In a single dice throw, $P(\text{'6'}) = \frac{1}{6}$. $P(\text{not '6'}) = \frac{5}{6}$

$$P(\text{three '6'}) = C_3^7 (\tfrac{1}{6})^3 (\tfrac{5}{6})^4 = \boxed{\frac{21875}{279936}}$$

Problem 47. In Minecraft, an end portal consists of 12 end portal frames, and each individual end portal frame has a 10% chance of naturally generating an ender eye in it (independent of other end portal frames). What is the probability that an end portal has 3 or more naturally generated ender eyes? (Express the answer as a percentage, correct to two decimal places.)

(Difficulty level: 7)

Solution 47. We can calculate the probability of having 0 eyes, 1 eyes and 2 eyes first.

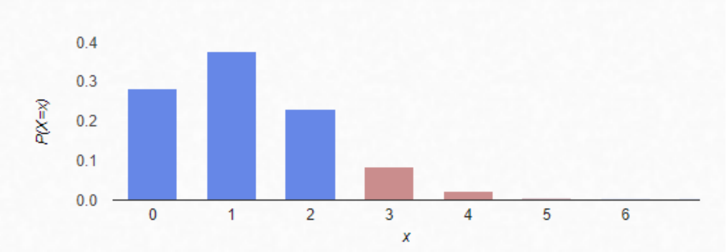
$P(0 \text{ eyes}) = C_0^{12} \cdot (0.9)^{12} \approx 28.24\%$

$P(1 \text{ eyes}) = C_1^{12} \cdot (0.9)^{12} \approx 37.66\%$

$P(\text{no eyes}) = C_2^{12} \cdot (0.1)^2(0.9)^{10} \approx 23.01\%$

$$\begin{aligned} P(3 \text{ eyes or more}) &= 1 - P(0 \text{ eyes}) - P(1 \text{ eyes}) - P(2 \text{ eyes}) \\ &\approx 1 - 28.24\% - 37.66\% - 23.01\% \\ &\approx \boxed{11.09\%} \end{aligned}$$

Discussion 47. Unfortunately, there is not a faster method to calculate this probability. So optimally, we will let a computer to do the work for us. The probability distribution of the number of eyes is as follows:

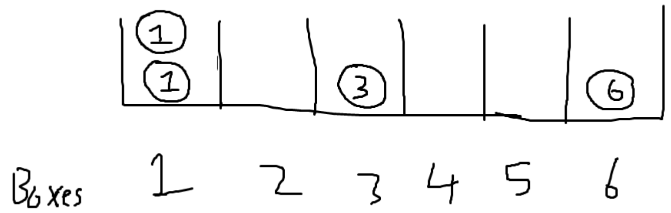


2.4 Unordered sampling with replacement

This case is the most complicated one among the four sampling types, and also the rarest one. It commonly arises when putting a fixed number of identical objects in a fixed number of distinct boxes, and summing up the numbers obtained when throwing a dice for a fixed number of times.

For example, suppose that I have an unlimited supply of 6 types of balls, each with the number '1', '2', '3', '4', '5', '6'. How many ways can I draw 4 balls without regard to order? I can draw '1' four times, or maybe I can draw ‘1’ two times and ‘3’, ‘4’ one time each. The sequences of draws (1, 1, 3, 6) and (6, 1, 3, 1) are consider the same way to draw the balls, but (1, 1, 1, 4) and (4, 4, 4, 1) are different.

We can make six boxes labelled from ‘1’ to ‘6’ each and line them up closely in a row, in ascending/descending order. Then we put all ‘1’ balls into box ‘1’, all ‘2’ balls into box ‘2’, and so on, like in the diagram.



The order of the balls within the same box does not matter, and only the amount of balls in the box matter. So the number of ways to draw the balls without order is the same as the number of ways to put the balls in the boxes.

Now if I remove the number on all the balls (but not the boxes), so that each card is identical, the number of ways to put the balls into the boxes is still the same. This is because the label on the boxes and the amount of identical balls already uniquely identify each way to put balls into the boxes.

We can count the walls between the balls placed in different boxes. (The right-wall of box ‘1’ and left-wall of box ‘2’ is counted as one wall) . The leftmost and rightmost wall of the boxes are not counted since they are not between any two balls. We can use identical stars * to represent the balls and identical bars | to represent the walls. So the balls (1, 1, 3, 6) can be represented as:

$$* * | | * | | | *$$

The number of ways to put the balls into the boxes is the same as the number of ways to arrange the stars and bars, because every way to put the balls into the boxes can be represented by a unique arrangement of stars and bars. And for every arrangement of stars and bars, there is only one unique way to put the balls into the corresponding boxes. Each time we swap a star and a bar, we are moving a card to a different box. If we swap two stars or swap two bars, they still account for the same way to put the balls into the boxes.

Thus, the number of ways to draw 4 balls without order and with repetition allowed is $C_4^{4+6-1} = C_4^9$. In general,

Theorem 2.7. If repetition is allowed and order does not matter, the total number of ways to choose k objects from a set with n elements is

$$C_k^{n+k-1} = \frac{(n+k-1)!}{k! \cdot (n-1)!}$$

Note that k can be larger or smaller than n in this case.

Also note that the number of ways to put k identical objects into n distinct boxes is also given by this formula, as we have shown in the example above. We can denote the number of balls in each box by x_i. Thus, we have the equation:

$$x_1 + x_2 + x_3 + \ldots + x_n = k \text{ , where } 0 \leq \ x_i \ \leq k \text{ and } x \in \mathbb{N}$$

We can see that the total number of non-negative integer solutions to this equation is the same as the number of ways to put k identical objects into n distinct boxes.

Problem 48. I throw a fair dice 5 times. What is the probability that the sum of the 5 numbers thrown is 10?

(Difficulty level: 7)

Solution 48. Let x_i be the number thrown in the ith throw. Each x_i must be an integer between 1 and 6 inclusive. We have

$$x_1 + x_2 + x_3 + x_4 + x_5 = 10 \text{ , where } 1 \leq x_i \leq 6$$

For the number of desired outcomes, we need to find the total number of integer solutions to this equation.

This is equivalent to the number of ways of putting 10 identical balls into 5 distinct boxes, in which each box must have at least 1 ball. First, we put one ball into each box and 'lock' them to satisfy the condition. After that, there are 5 balls remaining, which can be freely distributed among the 5 boxes. The number of ways the free balls are distributed can be solved using stars and bars (by only considering the free balls).

For example, if the sequence of numbers thrown is (2, 3, 1, 1, 3), the number of free balls distributed into each box is (1, 2, 0, 0, 2). It can be represented as * |** | | | ** .

Number of desired outcomes $= C_4^9$

Number of possible outcomes $= 6^5$

$$P(\text{sum to } 10) = \frac{C_4^9}{6^5} = \frac{126}{7776} = \boxed{\frac{7}{432}}$$

2.5 Inclusion-exclusion principle

Sometimes, when we have multiple events in the same sample space, they may overlap with each other. Let's say there are 7 balls put in a row, labelled from '1' to '7' each. Initially, they are in the order '1234567', and now I randomly arrange them. A_1 is the event that ball '1' is in its original position (1st position). A_2 is the event that ball '2' is in its original position (2nd position). A_1 and A_2 can happen at the same time, like the arrangement '1265743' . There can also be only one of them happening, like the arrangement '1365742'. The number of ways that both A_1 and A_2 happens is easy to find. Simply fix '12' at the front and arrange the rest, so there are 5! ways that it can happen.

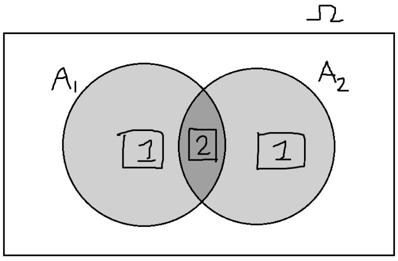
What if we want to find the number of ways that either A_1 or A_2 happens? No worries. We have the addition rule:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

First we find $|A_1|$ and $|A_2|$. For $|A_1|$, we fix '1' at the 1st position and arrange the rest, so $|A_1| = 6!$. Similarly, $|B_1| = 6!$. We have just found that $|A_1 \cap A_2| = 5!$. So $|A_1 \cup A_2| = 6! + 6! - 5! = 1320$

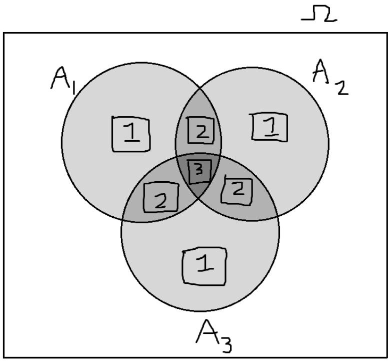
What if we want to find the number of ways that neither A_1 nor A_2 happens? This is $|(A_1 \cup A_2)'|$, and the total number of ways to arrange the 7 balls is $|\Omega| = 7!$. So $|(A_1 \cup A_2)'| = 7! - 1320 = 2640$

The addition rule can be illustrated with a Venn diagram.

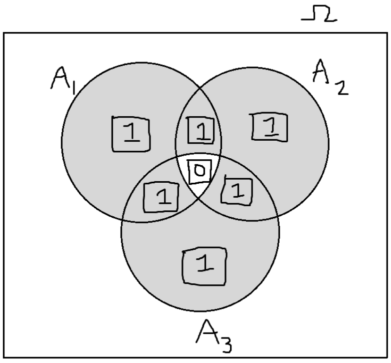


The number in the square represents how many times that region has been counted when we add $|A_1|$ and $|A_2|$. We want to count the region exactly once anywhere inside the circle, so we subtracted the common region $|A \cap B|$.

Now let A_i be the event that ball i is in the i th position. What if we need to find the number of ways that any of the balls '1', '2', '3' are in their original position? This is $|A_1 \cup A_2 \cup A_3|$. Similar to the two-event situation, we can add $|A_1|$, $|A_2|$ and $|A_3|$ first. $|A_1|+|A_2|+|A_3| = 6! = 2160$. However, we have double counted the cases that both A_1 and A_2 happen. Similarly, we have also double counted the cases that both A_2 and A_3 happen and the cases that both A_1 and A_3 happen. Moreover, we have triple counted the cases that both A_1, A_2, and A_3 happen. This can be illustrated with a Venn diagram.



So we subtract those. $|A_1 \cap A_2| = |A_2 \cap A_3| = |A_1 \cap A_3| = 5!$. So $2160 - 5! \times 3 = 1800$. After we subtract those, the diagram becomes:



We have subtracted one time too much for $|A_1 \cap A_2 \cap A_3|$, so we add it back. $|A_1 \cap A_2 \cap A_3| = 4!$. So $1800 + 4! = 1824$

Therefore, $|A_1 \cup A_2 \cup A_3| = 1824$

This method works for any 3 events A, B, C. We have

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$$

What about when there are 4 events or more? Maybe it will follow a similar pattern of alternately adding and subtracting terms.

Notations

Let $\sum\limits_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}|$denote the sum of number of elements of every unique 2-event intersections among the n events. So the number of ways to choose A_{i_1}, A_{i_2} from the n events is C^n_2. The notations for 3 and more events are similar. For k-event intersections, the notation is $\sum\limits_{1\leq i_1 \models i_k \leq n} |A_{i_1} \cap \ldots \cap A_{i_k}|$

Preposition. If there are n events labelled $A_1, A_2, \ldots, A_i$, then

$$\begin{aligned}|\bigcup_{i=1}^{n} A_i| = &\sum_{i=1}^{n} |A_i| - \sum_{1\leq i_1<i_2\leq n} |A_{i_1} \cap A_{i_2}| \\ &+ \sum_{1\leq i_1<i_2<i_3\leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\ &- \ldots + (-1)^{n-1} |\bigcap_{i=1}^{n} A_i|\end{aligned}$$

Let's use mathematical induction. (Ah shit, here we go again...)

Proof of inclusion-exclusion principle [9]

For all positive integers n, let $S(n)$ be the statement above. $S(1)$ is true, as that just says $|A_1| = |A_1|$

$S(2)$ is the statement $|A_1 \cup A_2| = |A| + |B| - |A \cap B|$, which is the addition rule, so $S(2)$ is also true.

Assume that $S(r)$ is true for some integer $r \geq 2$.

$$\begin{aligned}|\bigcup_{i=1}^{r} A_i| = &\sum_{i=1}^{r} |A_i| - \sum_{1\leq i_1<i_2\leq r} |A_{i_1} \cap A_{i_2}| \\ &+ \sum_{1\leq i_1<i_2<i_3\leq r} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\ &- \ldots + (-1)^{r-1} \sum_{1\leq i_1 \models i_{r-1} \leq r} |A_{i_1} \cap \ldots \cap A_{i_{r-1}} \cap A_{r+1}| \\ &+ (-1)^{r-1} |\bigcap_{i=1}^{r} A_i|\end{aligned}$$

$$\begin{aligned}\text{When } n = r+1, \text{ LHS} &= |\bigcup_{i=1}^{r+1} A_i| && (1)\\ &= |\bigcup_{i=1}^{r} A_i \cup A_{r+1}| && (2)\\ &= |\bigcup_{i=1}^{r} A_i| + |A_{r+1}| - |\bigcup_{i=1}^{r} A_i \cap A_{r+1}| \text{ (Addition rule)} && (3)\end{aligned}$$

Consider $|\bigcup_{i=1}^{r} A_i \cap A_{r+1}|$.

$$|\bigcup_{i=1}^{r} A_i \cap A_{r+1}| = |\bigcup_{i=1}^{r} (A_i \cap A_{r+1})| \qquad \text{(Generalized distributive law)} \tag{4}$$

By induction hypothesis,

$$\begin{aligned}
|\bigcup_{i=1}^{r} (A_i \cap A_{r+1})| = &\sum_{i=1}^{r} |A_i \cap A_{r+1}| && (5)\\
&- \sum_{1 \le i_1 < i_2 \le r} |A_{i_1} \cap A_{i_2} \cap A_{r+1}| && (6)\\
&+ \sum_{1 \le i_1 < i_2 < i_3 \le r} |A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{r+1}| && (7)\\
&- \ldots + (-1)^{r-1} |\bigcap_{i=1}^{r} A_i \cap A_{r+1}| && (8)
\end{aligned}$$

Thus, by expanding the first and last term in (3) with induction hypothesis,

$$\begin{aligned}
\text{LHS} = &\sum_{i=1}^{r} |A_i| && (9)\\
&- \sum_{1 \le i_1 < i_2 \le r} |A_{i_1} \cap A_{i_2}| && (10)\\
&+ \sum_{1 \le i_1 < i_2 < i_3 \le r} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| && (11)\\
&- \ldots + (-1)^{r-1} |\bigcap_{i=1}^{r} A_i| && (12)\\
&+ |A_{r+1}| && (13)\\
&- \sum_{i=1}^{r} |A_i \cap A_{r+1}| && (14)\\
&+ \sum_{1 \le i_1 < i_2 \le r} |A_{i_1} \cap A_{i_2} \cap A_{r+1}| && (15)\\
&- \sum_{1 \le i_1 < i_2 < i_3 \le r} |A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{r+1}| && (16)\\
&+ \ldots && (17)\\
&- (-1)^{r-1} |\bigcap_{i=1}^{r} A_i \cap A_{r+1}| && (18)
\end{aligned}$$

Rearranging the terms by pairing up the same number-intersections,

$$
\begin{aligned}
&\text{LHS}\\
&= \Big(\sum_{i=1}^{r} |A_i|\Big) + |A_{r+1}| && (19)\\
&\quad - \Big(\sum_{1\le i_1<i_2\le r} |A_{i_1}\cap A_{i_2}| + \sum_{i=1}^{r} |A_i \cap A_{r+1}|\Big) && (20)\\
&\quad + \sum_{1\le i_1<i_2<i_3\le r} |A_{i_1}\cap A_{i_2}\cap A_{i_3}| + \sum_{1\le i_1<i_2\le r} |A_{i_1}\cap A_{i_2}\cap A_{r+1}| && (21)\\
&\quad - \ldots && (22)\\
&\quad + (-1)^r \sum_{1\le i_1 ⧦ i_{r-1}\le r} |A_{i_1}\cap \ldots \cap A_{i_{r-1}}| + (-1)^r \sum_{1\le i_1 ⧦ i_{r-2}\le r} |A_{i_1}\cap \ldots \cap A_{i_{r-2}} \cap A_{r+1}| && (23)\\
&\quad + (-1)^{r-1} \bigcap_{i=1}^{r} |A_i| \quad + \quad (-1)^{r-1} \sum_{1\le i_1 ⧦ i_{r-1}\le r} |A_{i_1}\cap \ldots \cap A_{i_{r-1}} \cap A_{r+1}| && (24)\\
&\qquad\qquad + (-1)^r \,\Big|\bigcap_{i=1}^{r+1} A_i\Big| && (25)
\end{aligned}
$$

Note that (19) accounts for all the numbers of elements (/cardinalities) of single events from 1 to $r+1$.

In (20), the left term includes all the two-intersection cardinalities from 1 to r, and the right term includes all the two-intersection cardinalities where the higher index equals $r+1$. These two sums thus account for all possible two-intersection probabilities from 1 to $n+1$. To verify, there are C_2^r ways to pick 2 events from r events, and C_1^r ways to pick 2 events from $r+1$ events with one of the picked events locked to A_{r+1}. By the pascal's identity, $C_k^r + C_{k-1}^r = C_k^{r+1}$. So the sum of the two terms must be the number of ways to pick 2 events from $r+1$ events.

Similarly, in (21), the left term includes all three-intersection probabilities from 1 to r, and the right term includes those with highest index equal to $r+1$. Together they include all three-intersection probabilities from 1 to $r+1$.

This continues to (24), which together give all r-intersection cardinalities from 1 to $r+1$. Finally, we write down the last term, and

$$\begin{aligned}
&\text{LHS}\\
&=(\sum_{i=1}^{r+1}|A_i|) && (26)\\
&-\sum_{1\leq i_1<i_2\leq r+1}|A_{i_1}\cap A_{i_2}| && (27)\\
&+\sum_{1\leq i_1<i_2<i_3\leq r+1}|A_{i_1}\cap A_{i_2}\cap A_{i_3}| && (28)\\
&-\dots && (29)\\
&+(-1)^{r-1}\sum_{1\leq i_1 \vDash i_r\leq r+1}|A_{i_1}\cap\dots\cap A_{i_{r-1}}\cap A_{r+1}| && (30)\\
&+(-1)^r\ |\bigcap_{i=1}^{r+1}A_i| && (31)\\
&=\text{RHS} && (32)
\end{aligned}$$

$\therefore S(r+1)$ is true.
$\therefore$ By mathematical induction, $S(n)$ is true for all positive integers n. □

That was a tough one. To summarize, to count the number of elements of the union of all events, we first add the number of elements of individual events together, then subtract number of elements of any 2-intersection of events, then add back number of elements of any 3-intersection of events, and so on. For the number of k-intersection of events, if k is odd, then add. If k is even, then subtract.

Theorem 2.8. The inclusion-exclusion principle states that if there are n events labelled $A_1, A_2, \dots, A_i$, then

$$\begin{aligned}
|\bigcup_{i=1}^{n}A_i| &= \sum_{i=1}^{n}|A_i| - \sum_{1\leq i_1<i_2\leq n}|A_{i_1}\cap A_{i_2}|\\
&+\sum_{1\leq i_1<i_2<i_3\leq n}|A_{i_1}\cap A_{i_2}\cap A_{i_3}|\\
&-\dots+(-1)^{n-1}|\bigcap_{i=1}^{n}A_i|
\end{aligned}$$

The probability version of the inclusion-exclusion principle is similar:

If there are n events labelled $A_1, A_2, \ldots, A_i$, then

$$
\begin{aligned}
P(\bigcup_{i=1}^{n} A_i) =& \sum_{i=1}^{n} P(A_i) - \sum_{1\le i_1<i_2\le n} P(A_{i_1} \cap A_{i_2}) \\
&+ \sum_{1\le i_1<i_2<i_3\le n} P(A_{i_1} \cap A_{i_2} \cap A_{i_3}) \\
&- \ldots + (-1)^{n-1} P(\bigcap_{i=1}^{n} A_i)
\end{aligned}
$$

Let's get to the practical problems.

2.6 Derangements

Now we can finally answer the problem of the number of ways that the arranged balls go back to their original positions.

Problem 49. Seven balls labelled from '1' to '7' each are put in a row in ascending order of their numbers. Now I randomly arrange the balls. What is the probability that none of the balls go back to their original positions?

(Difficulty level: 8)

Solution 49. To find the number of ways that none of the balls go back to their original positions, we can first find the number of ways that any of the 7 balls go back to their original positions, then take the complement.

Let A_i denote the event that ball i goes back to its original position after arrangement. By the inclusion-exclusion principle,

$$
\begin{aligned}
|\bigcup_{i=1}^{7} A_i| =& \sum_{i=1}^{7} |A_i| - \sum_{1\le i<j\le 7} |A_i \cap A_j| \\
&+ \sum_{1\le i<j<k\le 7} |A_i \cap A_j \cap A_k| \\
&- \ldots + |\bigcap_{i=1}^{7} A_i| \\
=& C_1^7 \times 6! - C_2^7 \times 5! + C_3^7 \times 4! - C_4^7 \times 3! \\
&+ C_5^7 \times 2! - C_6^7 \times 1! + C_7^7 \times 0! \\
=& 3186
\end{aligned}
$$

$$P(\text{no balls back to original position})$$
$$= 1 - \frac{3186}{7!} = \boxed{\frac{103}{280}}$$

The permutation in which no balls go back to their original positions is called a **derangement**. Is there a faster way to calculate the total number of derangements of n balls? There seems to be some kind of pattern in the equation. Maybe we can get a general formula.

2.6.1 Derangement formula

Let there be n distinct objects put into n distinct positions. Let D_n be the number of derangements (/**derangement number** of n) and N be the number of ways of arranging the n objects such that at least one object goes into its original position.

Let A_i be the set of permutations in which the ith objecct goes back into its original position. Let's find $N = |\bigcup_{i=1}^{n}|$ first. Observe that $|A_i| = (n-1)!$ because we fix the position of one object and arrange the rest of the $n-1$ objects. Similarly, $|A_i \cap A_j| = (n-2)!$ objects because we fix the position of two objects and arrange the rest. So the number of permutations that k-set intersection contains is $(n-k)!$. We also know that there are C_k^n unique k-intersections from n sets since intersection is unordered and doesn't allow repeat.

From the inclusion-exclusion principle, we know that [10]

$$\begin{aligned}N = |\bigcup_{i=1}^{n} A_i| =& \sum_{i=1}^{n} |A_i| - \sum_{1\le i_1<i_2\le n} |A_{i_1} \cap A_{i_2}| + \sum_{1\le i_1<i_2<i_3\le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\ & - \ldots + (-1)^{n-1} |\bigcap_{i=1}^{n} A_i| \\ =& C_1^n (n-1)! - C_2^n (n-2)! + C_3^n (n-3)! - \ldots + C_n^n (n-n)! \\ =& \sum_{r=1}^{n} (-1)^{r+1} C_r^n (n-r)!\end{aligned}$$

(I use the variable 'r' because 'i' is too similar to '!' .)

Note that $C_r^n = \dfrac{n!}{r!\,(n-r)!}$.

$$= \sum_{r=1}^{n} (-1)^{r+1} \frac{n!}{r!}$$

Therefore, the number of derangements is

$$\begin{aligned} D_n &= n! - N \\ &= n! - \sum_{r=1}^{n} (-1)^{r+1} \frac{n!}{r!} \\ &= n! \left(1 + \sum_{r=1}^{n} (-1)^r \frac{1}{r!} \right) \\ &= n! \left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{1}{n!} \right) \\ &= n! \sum_{r=0}^{n} (-1)^r \frac{1}{r!} \qquad\qquad\qquad \ldots (1) \end{aligned}$$

We are not done yet. Importing our knowledge from Calculus, we know that there is a formula involving **Euler's number** e [10]:

$$e^{-1} = \sum_{r=0}^{\infty} (-1)^r \frac{1}{r!} \;=\; \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots$$

.The derangement formula looks awfully similar to the infinite series (Maclaurin series to be specific) expansion of e^{-1}. Maybe it has something to do with it?

First let me explain why e^{-1} can be written as that series. The definition of e is

$$e = \lim_{n \to \infty} (1 + \frac{1}{n})^n$$

Taking the natural log of both sides,

$$\begin{aligned} \ln e &= \ln \big(\lim_{n \to \infty} (1 + \frac{1}{n})^n \big) \\ 1 &= \lim_{n \to \infty} \ln (1 + \frac{1}{n})^n \qquad \text{(We can switch ln and lim.)} \end{aligned}$$

Multiplying by a constant x in both sides,

$$\begin{aligned} x &= x \lim_{n \to \infty} \ln (1 + \frac{1}{n})^n \\ x &= \lim_{n \to \infty} \ln (1 + \frac{1}{n})^{nx} \end{aligned}$$

[10] The value of $e \approx 2.718281828$

Let's do a change in variable $n = \dfrac{u}{x}$. When $n \to \infty$, $u \to \infty$.

$$x = \lim_{u\to\infty} \ln{(1+\frac{x}{u})^{(\frac{u}{x})\,x}}$$

$$x = \lim_{u\to\infty} \ln{(1+\frac{x}{u})^{u}}$$

Since u is a dummy variable, we can let back $n = u$. Also, we raise e to the power of both sides.

$$e^x = e^{\lim\limits_{n\to\infty} \ln{(1+\frac{x}{n})^{n}}}$$

$$e^x = e^{\ln{(\lim\limits_{n\to\infty}(1+\frac{x}{n})^{n})}}$$

$$\text{Since } e^{\ln(a)} = a, \qquad e^x = \lim_{n\to\infty}(1+\frac{x}{n})^n \qquad \dots(2)$$

Expanding the term inside the limit using binomial theorem, [11]

$$(1+\frac{x}{n})^n = \sum_{k=0}^{n} C_k^n (\frac{x}{n})^k = \sum_{k=0}^{n} x^k\,(C_k^n \frac{1}{n^k}) \qquad \dots(*)$$

$$\begin{aligned}
\text{Note that } C_k^n \frac{1}{n^k} &= \left(\frac{1}{n^k}\right)\left(\frac{n(n-1)(n-2)\dots(n-k+1)\,(n-k)!}{k!(n-k)!}\right) \\
&= \left(\frac{1}{k!}\right)\left(\frac{n(n-1)(n-2)\dots(n-k+1)}{n^k}\right) \\
&= \left(\frac{1}{k!}\right)\left(\frac{n}{n}\right)\left(\frac{n-1}{n}\right)\left(\frac{n-2}{n}\right)\dots\left(\frac{n-k+1}{n}\right) \\
&= \left(\frac{1}{k!}\right)(1)\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\dots\left(1-\frac{k-1}{n}\right)
\end{aligned}$$

Now let $n \to \infty$ in (*).

$$\begin{aligned}\lim_{n=\infty}(1+\frac{x}{n})^n &= \lim_{n=\infty}\sum_{k=0}^{n}\left(\frac{x^k}{k!}\right)\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{k-1}{n}\right)\\ &= \sum_{k=0}^{\infty}\lim_{n=\infty}\left[\left(\frac{x^k}{k!}\right)\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{k-1}{n}\right)\right]\\ &= \sum_{k=0}^{\infty}\left[\left(\frac{x^k}{k!}\right)(1-0)(1-0)\ldots(1-0)\right]\\ &= \sum_{k=0}^{\infty}\left(\frac{x^k}{k!}\right)\end{aligned}$$

Since $e^x = \lim_{n\to\infty}(1+\dfrac{x}{n})^n$, we have $e^x = \displaystyle\sum_{k=0}^{\infty}\left(\frac{x^k}{k!}\right)$. $\ldots$ (3)

Substituting $x=-1$, we get

$$e^{-1} = \sum_{k=0}^{\infty}(-1)^k\,\frac{1}{k!} \;=\; \frac{1}{0!}-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\ldots$$

.We finally justified this formula (or maybe not, as the sum rule and product rule of limits have not been justified, but nobody's got time for that). Now we can proceed by comparing $n!\,e^{-1} = \frac{n!}{e}$ and D_n side by side:

$$\begin{aligned}&D_n = n!\,\left(\frac{1}{0!}-\frac{1}{1!}+\frac{1}{2!}-\ldots+(-1)^n\,\frac{1}{n!}\right)\\ &\frac{n!}{e} = n!\,\left(\frac{1}{0!}-\frac{1}{1!}+\frac{1}{2!}-\ldots+(-1)^n\,\frac{1}{r!}+(-1)^{n+1}\,\frac{1}{(n+1)!}+(-1)^n\,\frac{1}{(n+2)!}+\ldots\right)\end{aligned}$$

The difference is [12]

$$\begin{aligned}\frac{n!}{e}-D_n &= n!\,\left((-1)^{n+1}\,\frac{1}{(n+1)!}+(-1)^n\,\frac{1}{(n+2)!}+\ldots\right)\\ &= \left((-1)^{n+1}\,\frac{1}{n+1}+(-1)^n\,\frac{1}{(n+1)(n+2)}+\ldots\right)\\ &= (-1)^{n+1}\left(\frac{1}{n+1}-\frac{1}{(n+1)(n+2)}+\frac{1}{(n+1)(n+2)(n+3)}-\ldots\right)\end{aligned}$$

The absolute difference between $\frac{n!}{e}$ and D_n (for $n \geq 2$) is:

$$\begin{aligned}
\left|D_n - \frac{n!}{e}\right| &= \frac{1}{n+1} - \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} - \cdots \\
&< \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \cdots \\
&< \frac{1}{n+1} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + \cdots \\
&= \frac{\frac{1}{n+1}}{1 - \frac{1}{n+1}} \qquad\qquad \text{(geometric series formula)} \\
&= \frac{1}{n}
\end{aligned}$$

Thus, $\left|D_n - \frac{n!}{e}\right| < \frac{1}{n}$ for all $n \geq 2$. The largest possible absolute difference for $n \geq 2$ is still smaller than $\frac{1}{2}$ when $n = 2$. Therefore, we have

$$D_n - \frac{1}{2} \; < \; \frac{n!}{e} \; < \; D_n + \frac{1}{2}$$

.Since D_n must be an integer, that means that the nearest integer that $\frac{n!}{e}$ rounds to must be D_n. This is important, because we have just discovered a much faster way for calculating D_n for $n \geq 2$, if we can get our hands on an ordinary scientific calculator (since it has the e button). Let $[\,a\,]$ denote the 'round off' function of a, which rounds a to the nearest integer (this has nothing to do with the square brackets we have used before). Then we have

$$D_n = \left[\frac{n!}{e}\right] \tag{4}$$

As for D_0 and D_1, using the old derangement formula (1) that we have shown before gives us $D_0 = 1,\ D_1 = 0$. Using this new formula (4), we get

$$\left[\frac{0!}{e}\right] = \left[\frac{1!}{e}\right] \approx [0.368] = 0$$

, so it works for D_1 but not D_0.

Thus, we have the derangement formulas:

Theorem 2.9. The total number of derangements of n distinct objects is (for $n > 0$):

$$D_n \;=\; n! \sum_{r=0}^{n} (-1)^r \, \frac{1}{r!} \;=\; \left[\frac{n!}{e}\right]$$

It follows from the theorem that the probability that n randomly arranged objects are deranged approaches $\frac{1}{e} \approx 36.79\%$ when $n \to \infty$.

Problem 50. In P.E. lesson, 23 students take turns to throw a sand bag on the playground without retrieving it immediately. After all of the students have thrown their sand bags, the students, one by one, randomly pick up one of the sand bags thrown on the playground. If John is one of the students, what is the probability that John is the only student who picks up the sand bags they have thrown themself?

(Difficulty: 8)

Solution 50. Whatever order that the students (including John) pick up the sand bags lead to the same required probability, as this situation is equivalent to randomly shuffling the sand bags among the students, so each permutation has an equal probability of occurring. Since only John's sand bag is fixed, none of the other 22 students get back their sand bags, so there are D_{22} desired outcomes. There are 23! permutations in total, so

$$\begin{aligned} &P(\text{only John picks up his sand bag }) \\ &= \frac{\left[\frac{22!}{e}\right]}{23!} = \boxed{\frac{6\,563\,440\,628\,747\,948\,887}{410\,349\,472\,045\,793\,280\,000}} \end{aligned}$$

2.6.2 Recursive derangement formula

What if the number of objects is even greater, such as 100? Then even a calculator cannot help us anymore when using this formula, since it will start to lose precision for the later digits because of floating point errors. Fortunately, there is a recursion formula that lets computers quickly generate the derangement numbers. [13]

Imagine deranging n objects (where $n \geq 2$). Let's call the object originally in the i th position 'object i'. Then the first object (object 1) can go to any of the last $n-1$ positions, which gives us $n-1$ choices. Suppose it goes to position k. We now have two options:

Option one: Object k goes to position 1 and we are left with the task of deranging the remaining $n-2$ objects. There are D_{n-2} ways to do this.

Option two: Object k does not go to positon 1. We are now left with the task of arranging $n-1$ objects (including object k) with each object having a single restriction: Object i cannot go to position i and object k cannot go to position 1. Since position k has been occupied by object 1 already, we can pretend that there are $n-1$ objects and positions to begin with by excluding old position k and old object 1. Then old object k becomes new object 1. We can see that this is the same as deranging $n-1$ objects in general, so there are D_{n-1} ways to do it.

The two options together show that there are $D_{n-2}+D_{n-1}$ ways to proceed once we have decided to send 1 to position k. Thus, we have the recursive formula

$$D_n = (n-1)(D_{n-2}+D_{n-1}) \tag{1}$$

The recursive formula is not as nice as we want since it involves D_{n-2}. Can we do better?

$$\begin{aligned} D_n &= (n-1)(D_{n-2}+D_{n-1}) \\ &= (n-1)D_{n-2}+nD_{n-1}-D_{n-1} \\ D_n - nD_{n-1} &= -(D_{n-1}-(n-1)D_{n-2}) \end{aligned}$$

The two sides look similar. The right hand side is just the negative of $n-1$ version of the left hand side. Also, we know the initial conditions $D_0 = 1$ and $D_1 = 0$. So

$$\begin{aligned} D_1 - 1D_0 &= 0-(1)(1) = -1 \\ D_2 - 2D_1 &= -(D_1 - 1D_0) = 1 \\ D_3 - 3D_2 &= -(D_2 - 2D_1) = -1 \\ D_4 - 4D_3 &= -(D_3 - 3D_2) = 1 \\ &\cdots \\ D_n - nD_{n-1} &= (-1)^n \\ D_n &= (-1)^n + nD_{n-1} \qquad (2) \end{aligned}$$

Thus, we have the theorem:

Theorem 2.10. Given the initial conditions $D_0 = 1$, $D_1 = 0$, the recursive formula for derangement number D_n is (for $n \geq 2$):

$$D_n = (n-1)(D_{n-2} + D_{n-1}) \tag{1}$$

$$D_n = (-1)^n + nD_{n-1} \tag{2}$$

Here's a python code to generate a list of derangement numbers from 0 to n.

```
def D(n):
    derangement_list = [0] * (n+1)
    derangement_list[0], derangement_list[1] = 1, 0
    for i in range(2, n+1):
        derangement_list[i] = (-1)**i + i * derangement_list[i-1]
    return derangement_list
```

The list of derangement numbers from 0 to 10 is:

n	0	1	2	3	4	5	6	7	8	9	10
$D(n)$	1	0	1	2	9	44	265	1854	14833	133496	1334961

2.6.3 Partial derangement

What if we want to find the number of ways that the first k of the n objects are deranged, but the rest of the objects are free to go where they want?

Problem 51. Twenty men check their hats into a cloak room. But the cloak boy is somewhat disorganized and forgets which hats belongs to whom and so, at the end of the evening, decides to hand the hats back to the gentlemen at random.

Ten of the men are lawyers. What is the probability that no lawyer gets his own hat back? (Express the answer as a percentage cor. to 2 d.p.)

(Difficulty level: 8) [13]

Solution 51. Let N be the number of ways that at least one of the lawyer gets his own hat back.

The number of ways that lawyer 1 gets his hat back is 19!. Same can be said for lawyer $2, 3, \ldots$. The number of ways that both lawyer 1 and lawyer 2 get their hat back is 18!. It is the same for any 2-combination of the 10 lawyers. The number of ways for 3 or more lawyers follows similar argument. By PIE (Principle of inclusion-exclusion),

$$\begin{aligned}N &= C_1^{10}19! - C_2^{10}18! + C_3^{10}17! - \ldots + C_{10}^{10}10! \\ &= 966944845408147200\end{aligned}$$

$$\begin{aligned}P(\text{no lawyer gets own hat back}) &= \frac{20! - 966944845408147200}{20!} \\ &= \boxed{60.26\%}\end{aligned}$$

Again, this can be generalized. When arranging n objects, let $D_{n,k}$ denote the ways that none of the first k are in their original position. Let N be the number of ways that at least one of the first k objects are in their original position. We have

$$\begin{aligned}D_{n,k} &= n! - N \\ &= n! - \sum_{r=1}^{k}(-1)^{r+1}C_r^k(n-r)! \\ &= (-1)^0\, C_0^k\, (n-0)! + \sum_{r=1}^{k}(-1)^r C_r^k(n-r)! \\ &= \sum_{r=0}^{k}(-1)^r C_r^k(n-r)!\end{aligned}$$

Theorem 2.11. The total number of derangements of k specific objects from n objects is (for $0 < k \leq n$):

$$D_{n,k} = \sum_{r=0}^{k}(-1)^r C_r^k(n-r)!$$

What if we want to find the number of ways that exactly k objects are deranged when arranging n objects? That means $n-k$ objects are fixed in their original position. There are C_k^n ways to choose which k objects to be deranged and fix the rest of $n-k$ objects. For the k objects chosen to be deranged, there are D_k ways to derange them. So the number of ways to derange exactly k objects is

$$D_k \times C_k^n$$

And the number of ways to derange at least k objects is

$$\sum_{i=k}^{n}(D_i \times C_i^n)$$

Note that $\sum_{i=0}^{n}(D_i \times C_i^n) = n!$, as any partial derangement must be one of the $n!$ permutations of objects.

Problem 52. A group of 8 friends are playing ‘Secret Santa’. First, each of them put their own gift (one gift for each person) in the middle of the room. Then, one by one, the gifts are randomly assigned back to one of the 8 friends who are not yet assigned a gift. What is the probability that 5 or more people do not get back their own gift?

(Difficulty level: 8)

Solution 52. Using the formula introduced above,

$$\begin{aligned}&P(5\text{ or more people do not get back their own gift})\\ =\ &\frac{D_5\,C_5^8 + D_6\,C_6^8 + D_7\,C_7^8 + D_8\,C_8^8}{8!} = \boxed{\frac{13183}{13440}}\end{aligned}$$

That’s enough derangements for today.

2.7 Other applications / non-applications of inclusion-exclusion principle

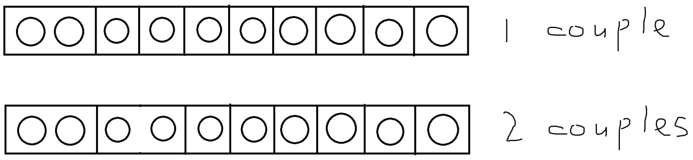
2.7.1 Multiple couples

Now we can tackle the challenging ‘movie seats’ problem.

Problem 53. Five couples go to the movies together. They randomly sit in a row of ten adjacent seats. What is the probability that nobody sits next to their partner?

(Difficulty level: 9) [14]

Solution 53. Let N_k denote the number of ways that k specific couples sit together (/sit next to their partner). Since the couples sit together, we can regard a couple as a single unit.



The number of ways that k specific couples sit together is $N_k = 2^k(10-k)!$. The 2^k in the formula is because we can order each partner within a unit in 2 ways, and there are k couple-units in total. The rest of the $10-2k$ people (individuals) may or may not sit next to their partner, and we can arrange them along with the couple-units. So the number of ways to arrange the individuals and couple-units (without regard to order within a unit) is $(k+(10-2k))! = (10-k)!$.

Since there are C^5_k ways to choose k couples from 5 couples, the number of ways that any k-combination of couples must sit together is $C^5_k \times N_k = C^5_k(2^k)(10-k)!$.

(Arbitrarily labelling the couples with a number.) Let A_i be the event that couple i sit together. By the inclusion-exclusion principle, the number of ways that at least 1 couple sits together is:

$$\begin{aligned}
|\bigcup_{i=1}^{5} A_i| =& \sum_{i=1}^{5} |A_i| - \sum_{1\le i<j\le 5} |A_i \cap A_j| + \sum_{1\le i<j<k\le 5} |A_i \cap A_j \cap A_k| \\
&- \sum_{1\le i<j<k<m\le 5} |A_i \cap A_j \cap A_k \cap A_m| + |\bigcap_{i=1}^{5} A_i| \\
=& \sum_{k=1}^{5} C^5_k(2^k)(10-k)! \\
=& 2365440
\end{aligned}$$

$$\begin{aligned}
&P(\text{nobody sits next to their partner}) \\
=& \frac{10! - 2365440}{10!} = \frac{1263360}{3628800} = \boxed{\frac{47}{135}}
\end{aligned}$$

2.7.2 Putting identical balls into distinct boxes with limited capacity / Sum of multiple dice throws

In Section 2.4, we've talked about how unordered sampling with replacement is equivalent to putting identical balls into distinct boxes. Now, what if I impose an extra restriction: Each box has a limited capacity and can only hold m balls at most. Can we still figure out the answer?

Problem 54. I throw a 4-sided fair dice 6 times. What is the probability the sum of the 6 numbers obtained is 15?

(Difficulty level: 8)

Solution 54. This situation is equivalent to putting 15 identical balls into 6 distinct boxes, where each box can hold at most 4 balls and each box must contain at least 1 ball. Fix one ball into each of the boxes. Now we have 9 free balls left. If there were no restrictions on the number of balls in each box, there would be $C_9^{9+6-1} = 2002$ ways to put the balls into the box. In these 2002 ways, let's first find out how many ways we can exceed the limit in at least one of the boxes.

Let A_i denote the event that the number of balls in box i exceeds the limit (greater than 4). To find $|A_1|$, we put 4 more balls into box 1 (so that there is 5 balls in box 1, thus ensured to exceed the limit) and fix them, then freely put the rest of the 5 balls into the boxes (including box 1). SO $|A_1| = C_5^{5+6-1} = 252$. Same can be said for other $|A_i|$ s. Now to find $|A_1 \cap A_2|$, we start with 9 free balls again, and fix 4 balls in box 1 and box 2 each. We put the remaining 1 ball freely into the boxes. $|A_1 \cap A_2| = C_1^{1+6-1} = 6$. There are no 3-event intersections or more (since there are not enough balls), so we can ignore these. Same can be said for other 2-intersections $|A_i \cap A_j|$. By the inclusion-exclusion principle,

$$\begin{aligned}
|\bigcup_{i=1}^{6} A_i| &= \sum_{i=1}^{6} |A_i| - \sum_{1\leq i<j\leq 6} |A_i \cap A_j| \\
&= C_1^6 \times 252 - C_2^6 \times 6 \\
&= 1422
\end{aligned}$$

So the number of ways that the number of balls does not exceed the limit in all boxes is $2002 - 1422 = 580$. This is also the number of desired outcomes number of ways to get 15 by summing up the numbers obtained by throwing a 4-sided dice 6 times. The total number of possible outcomes is 4^6.

$$\begin{aligned}
&P(\text{sum is 15}) \\
&= \frac{580}{4^6} = \boxed{\frac{145}{1024}}
\end{aligned}$$

In general, when putting k identical balls into n distinct boxes, where each box has a capacity of m and is allowed to be empty (thus differs from the case above), the number of way to put the balls into the boxes is

$$\begin{aligned}
&C_k^{n+k-1} - \sum_{r=1}^{n} (-1)^{r+1}\, C_r^n\, C_{n-1}^{k-r(m+1)+n-1} \\
&= (-1)^0\, C_0^n\, C_{n-1}^{k-0(m+1)+n-1} + \sum_{r=1}^{n} (-1)^r\, C_r^n\, C_{n-1}^{k-r(m+1)+n-1} \\
&= \sum_{r=0}^{n} (-1)^r\, C_r^n\, C_{n-1}^{k-r(m+1)+n-1}
\end{aligned}$$

Note that if $k < r(m+1)$ in the summation, then $C_{n-1}^{k-r(m+1)+n-1} = 0$, so the whole term is 0. This is consistent with how we have 'ignored' the terms of 3-and-more-intersection in the solution above. Thus, the formula can also be stated as

$$\sum_{0 \le r \le \frac{k}{m+1}} (-1)^r\, C_r^n\, C_{n-1}^{k-r(m+1)+n-1}$$

If every box must contain at least 1 ball, then there are $k-n$ free balls left. To exceed limit in a box, m more balls must be added to the box. This is also equivalent to rolling a m-sided dice for n times and the numbers obtained sum up to k . The number of ways to do this is:

$$\sum_{r=0}^{n} (-1)^r\, C_r^n\, C_{n-1}^{k-rm-1}$$

Plugging in the numbers in Problem 53, $m = 4$, $n = 6$, $k = 15$, we get the number of ways is 580, which is the same as the solution.

Theorem 2.12. The number of ways that a m-sided dice is rolled for n times and the numbers obtained sum up to k is:

$$\sum_{r=0}^{n} (-1)^r\, C_r^n\, C_{n-1}^{k-rm-1}$$

Problem 55. Peter has nine four-sided (pyramidal) dice, each with faces numbered 1, 2, 3, 4. Colin has six six-sided (cubic) dice, each with faces numbered 1, 2, 3, 4, 5, 6.

Peter and Colin roll their dice and compare totals: the highest total wins. The result is a draw if the totals are equal.

What is the probability that Pyramidal Pete beats Cubic Colin?

(Give your answer rounded to seven decimal places in the form 0.abcdefg)

(Difficulty level: 9) [15] (Project Euler Problem 205)

Solution 55. The probability distribution of the sum S_6 of the six 6-sided dice can be found with the formula (for $6 \leq k \leq 36$)

$$P(S_6 = k) = \frac{1}{6^6} \sum_{r=0}^{6} (-1)^r \, C_r^6 \, C_5^{k-6r-1}$$

Similarly, the probability distribution of the sum S_4 of the nine 4-sided dice can be found with the formula (for $9 \leq k \leq 36$)

$$P(S_4 = k) = \frac{1}{4^9} \sum_{r=0}^{9} (-1)^r \, C_r^9 \, C_8^{k-4r-1}$$

If given that the sum of the six 6-sided dice (Colin) is c, then the probability that the sum S_4 of the nine 4-sided dice (Pete) is larger than c is:

$$\begin{aligned} P(S_4 > c \,|\, S_6 = c) &= \sum_{k=c+1}^{36} P(S_4 = k) \\ &= \frac{1}{4^9} \sum_{k=c+1}^{36} (\sum_{r=0}^{9} (-1)^r \, C_r^9 \, C_8^{k-4r-1}) \end{aligned}$$

Thus,

$$\begin{aligned} P(S_4 > S_6) &= \sum_{c=6}^{36} P(S_4 > c \,|\, S_6 = c) P(S_6 = c) \\ &= \sum_{c=6}^{36} \left(\frac{1}{4^9} \sum_{k=c+1}^{36} (\sum_{r=0}^{9} (-1)^r \, C_r^9 \, C_8^{k-4r-1}) \right) \left(\frac{1}{6^6} \sum_{r=0}^{6} (-1)^r \, C_r^6 \, C_5^{c-6r-1} \right) \\ &= \frac{1}{(6^6)(4^9)} \sum_{c=6}^{36} \left(\sum_{k=c+1}^{36} (\sum_{r=0}^{9} (-1)^r \, C_r^9 \, C_8^{k-4r-1}) \right) \left(\sum_{r=0}^{6} (-1)^r \, C_r^6 \, C_5^{c-6r-1} \right) \end{aligned}$$

Using python to do the calculations for us:

```
import math
def bi(n,k):  # Binomial formula that returns 0 if k > n
    if k > n: return 0
    return math.comb(n,k)

def S6(k):    # Number of ways that S_6 = k
    res = 0
    for r in range(7):
        res += (-1)**r * bi(6,r) * bi(k-6*r-1,5)
    return res

def S4(k):    # Number of ways that S_4 = k
    res = 0
    for r in range(10):
        res += (-1)**r * bi(9,r) * bi(k-4*r-1,8)
    return res

def is_larger(c):   # Number of ways that S_4 > c
    res = 0
    for k in range(c+1,37):
        res += S4(k)
    return res

s = 0
for c in range(6,37):
    s += is_larger(c) * S6(c)
print( s/ (6**6 * 4**9))
```

And we get

```
0.5731440767829801
```

So the answer is

$$P(S_4 > S_6) = \boxed{0.5731441}$$

Problem 56.1. Four dice are thrown at the same time. What is the probability that the sum of the numbers obtained is divisible by 4?

(Difficulty level: 8)

Solution 56.1. The possible sums range from 4 to 24 inclusive, and the desired sums are 4, 8, 12, 16, 20, 24. Using the dice sum formula, the number of ways that the sum is divisible by 4 is:

$$\sum_{k=4,\ \text{step}=4}^{24} \left(\sum_{r=0}^{4} (-1)^r C_r^4 C_3^{k-6r-1}\right) = 322$$

The number of possible outcomes is $6^4 = 1296$. So

$P(\text{sum divisible by } 4) = \dfrac{322}{1296} = \boxed{\dfrac{161}{648}}$

Problem 56.2. Six dice are thrown at the same time. What is the probability that the sum of the numbers obtained is divisible by 7?

(Difficulty level: 8) [16]

Solution 56. We can pretend that it is the same dice thrown six times since it is an equivalent situation.

Let p_n be the probability that the sum of the numbers obtained so far is a multiple of 7 after n rolls.

Then we get the recursion:

$$p_{n+1} = \frac{1}{6}(1 - p_n)$$

This is because to get a multiple of 7 at roll $n + 1$, you have to get a non-multiple of 7 at roll n (with probability $1 - p_n$), and then get exactly the right value (with probability $\frac{1}{6}$). For example, if the sum is 13 after roll n, then there is a $\frac{1}{6}$ probability to get 1 in the next roll, making the sum 14.

Starting with $p_0 = 1$:

$$\begin{aligned} p_0 &= 1 \\ p_1 &= 0 \\ p_2 &= \frac{1}{6} \\ p_3 &= \frac{5}{36} \\ p_4 &= \frac{31}{216} \\ p_5 &= \frac{185}{1296} \\ p_6 &= \frac{1111}{7776} \end{aligned}$$

Thus, $P(\text{sum divisible by } 7) = \boxed{\dfrac{1111}{7776}}$

2.7.3 Putting distinct balls into distinct boxes with minimum/maximum requirements

Problem 57.1. 18 dice are thrown at the same time. What is the probability that each number shows up at least once?

(Difficulty level: 8)

Solution 57.1. There are 6^{18} possible outcomes. Let A_n be the event that the number n does not show up. The number of desired outcomes $S = 6^{18} - |\bigcup_{i=1}^{6} A_i|$. Note that there must be some number that appears at least once, so $|\bigcap_{i=1}^{6} A_i| = 0$.

Recall the inclusion-exclusion principle:

$$\begin{aligned}
|\bigcup_{i=1}^{6} A_i| =& \sum_{i=1}^{6} |A_i| - \sum_{1\le i<j\le 6} |A_i \cap A_j| + \sum_{1\le i<j<k\le 6} |A_i \cap A_j \cap A_k| \\
& - \ldots + \ldots - |\bigcap_{i=1}^{6} A_i| \\
6^{18} - S =& \sum_{i=1}^{6} |A_i| - \sum_{1\le i<j\le 6} |A_i \cap A_j| + \sum_{1\le i<j<k\le 6} |A_i \cap A_j \cap A_k| \\
& - \ldots + \ldots - 0 \\
S =& 6^{18} - \sum_{i=1}^{6} |A_i| + \sum_{1\le i<j\le 6} |A_i \cap A_j| - \sum_{1\le i<j<k\le 6} |A_i \cap A_j \cap A_k| \\
& + \ldots - \sum_{1\le i<j<k<l<m\le 6} |A_i \cap A_j \cap A_k \cap A_l \cap A_m|
\end{aligned}$$

Note that if there are k numbers that do not show up, then there are C_k^6 ways to choose the k events, and there are $6 - k$ numbers available for each dice, so the total number of ways that can happen is $C_k^6(6-k)^{18}$. Substituting values:

$$\begin{aligned}
S =& 6^{18} - C_1^6 \cdot 5^{18} + C_2^6 \cdot 4^{18} - C_3^6 \cdot 3^{18} + C_4^6 \cdot 2^{18} - C_5^6 \cdot 1^{18} \\
=& 79694820748080
\end{aligned}$$

$$\begin{aligned}&P(\text{At least one of each number})\\&=\frac{79694820748080}{6^{18}}\\&=\boxed{\frac{553436255195}{705277476864}}\end{aligned}$$

Problem 57.2. 18 dice are thrown at the same time. What is the probability that each number shows up at least twice?

(Difficulty level: 9)

Solution 57.2. If each number shows up at least twice, then the it is certain that some 12 dice will be in the form (2, 2, 2, 2, 2, 2) , where the i th element of this tuple indicates the number of times that the number i shows up in the 12 dice.

The numbers on the remaining 6 dice are free to be whatever they want, and the distinct formations (regarding each number on the dice as identical for simplicity) are the list of all partitions of the integer 6, namely:

(6, 0, 0, 0, 0, 0) , (5, 1, 0, 0, 0, 0) , (4, 1, 1, 0, 0, 0)
(4, 2, 0, 0, 0, 0) , (3, 1, 1, 1, 0, 0) , (3, 2, 1, 0, 0, 0)
(3, 3, 0, 0, 0, 0) , (2, 1, 1, 1, 1, 0) , (2, 2, 1, 1, 0, 0)
(2, 2, 2, 0, 0, 0) , (1, 1, 1, 1, 1, 1)

Adding the 12 dice that form (2, 2, 2, 2, 2, 2), we get the distinct formations of 18 dice:

(8, 2, 2, 2, 2, 2) , (7, 3, 2, 2, 2, 2) , (6, 3, 3, 2, 2, 2)
(6, 4, 2, 2, 2, 2) , (5, 3, 3, 3, 2, 2) , (5, 4, 3, 2, 2, 2)
(5, 5, 2, 2, 2, 2) , (4, 3, 3, 3, 3, 2) , (4, 4, 3, 3, 2, 2)
(4, 4, 4, 2, 2, 2) , (3, 3, 3, 3, 3, 3)

Now we regard each number as distinct, so (8, 2, 2, 2, 2, 2) and (2, 8, 2, 2, 2, 2) are different things. The number of ways that each formation can appear is:

Formation	Formula for Outcomes	Total Outcomes
(8, 2, 2, 2, 2, 2)	$C_1^6 \cdot \dfrac{18!}{8!(2!)^5}$	29772943200
(7, 3, 2, 2, 2, 2)	$P_2^6 \cdot \dfrac{18!}{7!\,3!(2!)^4}$	396972576000
(6, 3, 3, 2, 2, 2)	$6 \cdot C_2^5 \cdot \dfrac{18!}{6!\,(3!)^2(2!)^3}$	1852538688000
(6, 4, 2, 2, 2, 2)	$P_2^6 \cdot \dfrac{18!}{6!\,4!(2!)^4}$	694702008000
(5, 3, 3, 3, 2, 2)	$6 \cdot C_3^5 \cdot \dfrac{18!}{5!\,(3!)^3(2!)^2}$	3705077376000
(5, 4, 3, 2, 2, 2)	$P_3^6 \cdot \dfrac{18!}{5!\,4!\,3!(2!)^3}$	5557616064000
(5, 5, 2, 2, 2, 2)	$C_2^6 \cdot \dfrac{18!}{(5!)^2(2!)^4}$	416821204800
(4, 3, 3, 3, 3, 2)	$P_2^6 \cdot \dfrac{18!}{4!\,(3!)^4 2!}$	3087564480000
(4, 4, 3, 3, 2, 2)	$C_2^6 C_2^4 \cdot \dfrac{18!}{(4!)^2(3!)^2(2!)^2}$	6947020080000
(4, 4, 4, 2, 2, 2)	$C_3^6 \cdot \dfrac{18!}{(4!)^3(2!)^3}$	1157836680000
(3, 3, 3, 3, 3, 3)	$\dfrac{18!}{(3!)^6}$	137225088000
Total	—	23983147188000

The total is the number of desired outcomes. There are 6^{18} possible outcomes. So

$$P(\text{ at least 2 of each number}) = \frac{23983147188000}{6^{18}} = \boxed{\frac{83\,274\,816\,625}{352\,638\,738\,432}}$$

Discussion 57.2. The inclusion-exclusion principle is too difficult to apply in this case, so I used this method instead.

Problem 58.1. 10 four-sided dice are thrown at the same time. What is the probability that no number shows up 6 times or more?

(Difficulty level: 8)

Solution 58.1. It is slightly easier to first find the number of ways that some numbers show up 6 times or more. Let's regard the numbers as identical for convenience now. In that case, the formation of some 6 dice is $(6, 0, 0, 0)$. The numbers on the remaining 4 dice are free to be whatever they want, and the distinct formations are the list of all partitions of the integer 4, namely:

(4, 0, 0, 0) , (3, 1, 0, 0) , (2, 1, 1, 0) , (2, 2, 0, 0) , (1, 1, 1, 1)

Note that adding one of the (6, 0, 0, 0) or (0, 6, 0, 0) or (0, 0, 6, 0) or (0, 0, 0, 6) to the same partition may yield different distinct formations. By adding them to the list of partitions, we get all the distinct formations of 10 dice:

(10, 0, 0, 0) , (6, 4, 0, 0) , (9, 1, 0, 0) , (7, 3, 0, 0) , (6, 3, 1, 0)
(8, 1, 1, 0) , (7, 2, 1, 0) , (6, 2, 1, 1) , (8, 2, 0, 0) , (6, 2, 2, 0)
(7, 1, 1, 1)

Now we regard each number as distinct, so (6, 4, 0, 0) and (4, 6, 0, 0) are different things. The number of ways that each formation can appear is: (next page)

Formation	Formula for Outcomes	Total Outcomes
(10, 0, 0, 0)	C^4_1	4
(6, 4, 0, 0)	$P^4_2 \cdot \dfrac{10!}{6!\,4!}$	2520
(9, 1, 0, 0)	$6 \cdot P^4_2 \cdot \dfrac{10!}{9!}$	120
(7, 3, 0, 0)	$P^4_2 \cdot \dfrac{10!}{7!\,3!}$	1440
(6, 3, 1, 0)	$6 \cdot C^4_3 \cdot \dfrac{10!}{6!\,3!}$	20160
(8, 1, 1, 0)	$4 \cdot C^3_2 \cdot \dfrac{10!}{8!}$	1080
(7, 2, 1, 0)	$P^4_3 \cdot \dfrac{10!}{7!\,2!}$	8640
(6, 2, 1, 1)	$P^4_2 \cdot \dfrac{10!}{6!\,2!}$	30240
(8, 2, 0, 0)	$P^4_2 \cdot \dfrac{10!}{8!\,2!}$	540
(6, 2, 2, 0)	$4\ C^3_2 \cdot \dfrac{10!}{6!\,2!\,2!}$	15120
(7, 1, 1, 1)	$C^4_1 \dfrac{10!}{7!}$	2880
Total	—	82744

Thus, the desired number of ways that no number shows up times or more is $4^{10} - 82744 = 965832$.

$$P(\text{no number shows up 6 times or more})= \frac{965832}{4^{10}} = \boxed{\frac{120729}{131072}}$$

Problem 58.2. 18 dice are thrown at the same time. What is the probability that no number shows up 7 times or more?

(Difficulty level: 9)

Solution 58.2. This time, it is easier to directly count the number ways that any number only shows up at maximum of 6 times . Listing all the distinct desired formations out by hand is too troublesome, so I will use python to help me. First, make a function that spits out the list of all partitions of an integer. (I won't explain how it works because I don't know either.)

```
def partitions(n, I=1):
    yield (n,)
    for i in range(I, n//2 + 1):
        for p in partitions(n-i, i):
            yield (i,) + p
```

Then make a bunch of functions that will help give us the distinct desired formations.

```
import math, itertools
from collections import Counter

def pad(x, n): # pad 0s until list x is not shorter than length n
    res = x
    for i in range(n-len(x)):
        res.append(0)
    return res

def atmost(x,k): # check if all elements in list x are not larger than k
    if max(x)>k: return 0
    return 1

def f(n):  # A shorthand for n!
    return math.factorial(n)

def arran(x):   # number of ways to arrange the numbers in list x
    freq_list = Counter(x)
    s = f(len(x))
    for i in freq_list:
        s = s // ( f(freq_list[i]) )
    return s

def form(x, k):  # number of ways for the this formation to appear
# regarding each number as distinct
    s = f(k)
    for i in x:
        s = s // (f(i))
    return s

def partway(n,k, m): # number of ways that none of the k n-sided dice
# show up more than m times
    partition_list = list(partitions(k))
    partition_list = list(map(list, partition_list)  )
    partition_list = [pad(i,n) for i in partition_list]
    partition_list2 = []
    for i in partition_list:
        if len(i)<=n and atmost(i,m):
            partition_list2.append(i)
    partition_list = partition_list2.copy()
    partition_list = [sorted(i, reverse=True) for i in partition_list]
    partition_list = set([tuple(i) for i in partition_list])
    res = [arran(i) * form(i, k)  for i in partition_list]
    res2 = list(zip(partition_list, res))
    return res2 , f'total : {sum(res)}'

print(partway(6,18,6))
```

And we get

```
([((5, 3, 3, 3, 3, 1), 1235025792000),
  ((5, 4, 4, 3, 1, 1), 2778808032000),
  ((6, 5, 3, 2, 1, 1), 2223046425600),
  ((5, 4, 4, 2, 2, 1), 4168212048000),
  ((5, 5, 3, 2, 2, 1), 3334569638400),
  ((5, 5, 5, 3, 0, 0), 37050773760),
  ((5, 3, 3, 3, 2, 2), 3705077376000),
  ((6, 6, 2, 2, 1, 1), 277880803200),
  ((5, 5, 3, 3, 1, 1), 1111523212800),
  ((4, 3, 3, 3, 3, 2), 3087564480000),
  ((6, 5, 4, 2, 1, 0), 1111523212800),
  ((6, 6, 3, 3, 0, 0), 30875644800),
  ((6, 4, 4, 3, 1, 0), 926269344000),
  ((4, 4, 3, 3, 3, 1), 3087564480000),
  ((6, 6, 3, 1, 1, 1), 123502579200),
  ((6, 5, 3, 3, 1, 0), 741015475200),
  ((5, 5, 4, 3, 1, 0), 1111523212800),
((6, 6, 6, 0, 0, 0), 343062720),
((5, 4, 4, 4, 1, 0), 463134672000),
((4, 4, 4, 3, 2, 1), 4631346720000),
((4, 4, 4, 3, 3, 0), 771891120000),
((6, 5, 4, 1, 1, 1), 370507737600),
((6, 5, 4, 3, 0, 0), 185253868800),
((5, 5, 2, 2, 2, 2), 416821204800),
((6, 6, 5, 1, 0, 0), 18525386880),
((4, 4, 4, 2, 2, 2), 1157836680000),
((4, 4, 4, 4, 2, 0), 289459170000),
((4, 4, 3, 3, 2, 2), 6947020080000),
((6, 3, 3, 3, 2, 1), 2470051584000),
((6, 3, 3, 3, 3, 0), 205837632000),
((6, 4, 3, 2, 2, 1), 5557616064000),
((6, 6, 3, 2, 1, 0), 370507737600),
((5, 5, 4, 2, 1, 1), 1667284819200),
((6, 5, 2, 2, 2, 1), 1111523212800),
((6, 3, 3, 2, 2, 2), 1852538688000),
((5, 5, 4, 2, 2, 0), 833642409600),
((6, 4, 3, 3, 1, 1), 1852538688000),
((4, 4, 4, 4, 1, 1), 289459170000),
((6, 5, 5, 1, 1, 0), 111152321280),
((6, 4, 4, 2, 2, 0), 694702008000),
((6, 4, 3, 3, 2, 0), 1852538688000),
((5, 4, 3, 3, 3, 0), 1235025792000),
((5, 5, 4, 4, 0, 0), 69470200800),
((5, 4, 3, 3, 2, 1), 11115232128000),
((6, 5, 5, 2, 0, 0), 55576160640),
((6, 6, 2, 2, 2, 0), 92626934400),
((6, 6, 4, 1, 1, 0), 92626934400),
((6, 4, 4, 4, 0, 0), 38594556000),
((5, 4, 3, 2, 2, 2), 5557616064000),
((6, 5, 3, 2, 2, 0), 1111523212800),
((5, 5, 5, 2, 1, 0), 222304642560),
((6, 4, 4, 2, 1, 1), 1389404016000),
((6, 6, 4, 2, 0, 0), 46313467200),
((3, 3, 3, 3, 3, 3), 137225088000),
((5, 5, 5, 1, 1, 1), 74101547520),
((6, 4, 2, 2, 2, 2), 694702008000),
((5, 4, 4, 3, 2, 0), 2778808032000),
((5, 5, 3, 3, 2, 0), 1111523212800)],
 'total : 89035239252960')
```

The total 89035239252960 is the number of desired outcomes.

Thus, P(no number shows up 7 times or more)

$$= \frac{89035239252960}{6^{18}}$$

$$= \boxed{\frac{309150136295}{352638738432}}$$

Problem 59. 10 dice are thrown at the same time. What is the probability that exactly 3 distinct numbers show up on the dice?

(Difficulty level: 8)

Solution 59. Let's first calculate the number of ways (denoted S) for 3 particular numbers to appear at least once while the other 3 numbers never appear. By the inclusion-exclusion principle,

$S = 3^{10} - C_1^3 \cdot 2^{10} + C^2 \cdot 1^{10} = 55980$.

The number of ways to choose 3 particular numbers from 6 numbers is C_3^6 , so

P(exactly 3 distinct numbers)$= \dfrac{C_3^6 \cdot 55980}{6^{10}} = \dfrac{1119600}{60466176} = \boxed{\dfrac{7775}{419904}}$

2.8 Miscellaneous situations

(Let me introduce a notation:
Let $a \mathrel{|\!\!=\!\!|} b$ denote 'integers from a to b inclusive',
and $A_a \mathrel{|\!\!=\!\!|} A_b$ denote '$A_{a+1}, A_{a+2}, \ldots, A_{b-1}, A_b$' .)

2.8.1 Miscellaneous problems

Problem 60. Suppose three dice are thrown and let S denote the sum of the three numbers obtained. Given that $S \in \{9, 10, 11, 12\}$, what is the probability that $S = 10$ or $S = 11$?

(Difficulty level: 7) [2] (Classic Problems of Probability Q2 Modified)

Solution 60. We can count the number of possible outcomes for each sum with a table. Let (a, b, c) be the case of getting 'a', 'b', 'c' in any order.

$S = 12$	# of ways	$S = 11$	# of ways	$S = 10$	# of ways	$S = 9$	# of ways
$(6, 5, 1)$	6	$(6, 4, 1)$	6	$(6, 3, 1)$	6	$(6, 2, 1)$	6
$(6, 4, 2)$	6	$(6, 3, 2)$	6	$(6, 2, 2)$	3	$(5, 3, 1)$	6
$(6, 3, 3)$	3	$(5, 5, 1)$	3	$(5, 4, 1)$	6	$(5, 2, 2)$	3
$(5, 5, 2)$	3	$(5, 4, 2)$	6	$(5, 3, 2)$	6	$(4, 4, 1)$	3
$(5, 4, 3)$	6	$(5, 3, 3)$	3	$(4, 4, 2)$	3	$(4, 3, 2)$	6
$(4, 4, 4)$	1	$(4, 4, 3)$	3	$(4, 3, 3)$	3	$(3, 3, 3)$	1
Total	25	Total	27	Total	27	Total	25

$$P(S = 10 \text{ or } 11 \,|\, \{9 \text{⧦} 12\}) = \frac{27 + 27}{25 + 27 + 27 + 25} = \boxed{\frac{27}{52}}$$

Problem 61. There are 100 people in line to board a plane with 100 seats. The first person has lost his boarding pass, so he takes a random seat.

Everyone that follows takes their assigned seat if it's available, but otherwise takes a random unoccupied seat. What is the probability the last passenger ends up in his/her assigned seat?

(Difficulty level: 7) [3]

Solution 61. [17] The first person is equally likely to take every seat in the plane (including his assigned seat). Also note that (for $k > 1$) after the k th person boarded the plane, the k th seat must be either occupied by the k th person or by a person that randomly took the seat before k th person boarded the plane.

Look at the situation when the k th passenger enters. Neither of the previous passengers showed any preference for the k th seat vs. the seat of the first passenger. This in particular is true when $k = 100$. But the 100 th passenger can only occupy his seat or the first passenger's seat.

Therefore the probability is $\boxed{\frac{1}{2}}$.

2.8.2 Pairings of objects

Problem 62.1. In a class, there are 5 boys and 3 girls. The teacher randomly pairs up all the students. (This means the teacher randomly chooses two unpaired students and make them a pair. This process is repeated until all the students are paired up.) What is the probability that there are exactly 1 pair of students which consists of one boy and one girl?

(Difficulty level: 7)

Solution 62.1a. We can think of it as the teacher randomly arranges the students in a row and draws a line between every two students, like this:

There are 8! possible arrangements, so there are 8! ways to pair the students with regard to the order within each pair and the order among pairs.

For the desired pairings, there must be exactly 1 (B, G) pair, 2 (B, B) pairs and 1 (G, G) pair. One possible arrangement of students can be BB | BB | GG | BG . If the gender of students are in this order, then there are $P_2^5 P_2^3 = P_4^5$ ways to choose and arrange 4 boys from 5 boys to be the BB | BB in the front. The remaining boy will be in the 7th position.

Similarly, there are P_2^3 ways to choose and arrange 2 girls from 3 girls to be the GG after the boys. The remaining girl will be in the last position. So this exact order of gender has $P_4^5\, P_2^3 = 720$ ways to appear.

Now let's allow arrangements of genders. First, there are 2! ways to arrange the BG at the end of the line. Now we regard each (B,B) pair as identical since we have counted every order of boys among BB | BB already. There are $\frac{4!}{2!}$ to arrange the order that each pair appear, so the total number of ways that there is exactly 1 (B,G) pair is $720 \times 2! \times \frac{4!}{2!} = 17280$.

Thus $P(\text{exactly 1 pair of (B,G)}) = \dfrac{17280}{8!} = \boxed{\dfrac{3}{7}}$

Solution 62.1b. Notice that we counted all the possible orderings within and among the pairs in both the numerator and denominator of the probability, making the calculation more complicated than it needs to be.

If we count the number of possible pairings without regard to the order within each pair (but still with regard to order among the pairs), then there are C_2^8 ways to choose the students to be the 1st pair, and

C_2^6 for 2nd pair, C_2^4 for 3rd pair, and C_2^2 for 4th pair. So there are $C_2^8 C_2^6 C_2^4 C_2^2 = 2520$ such pairings.

If we don't care about the order that the pairs appear, then every 4! old pairs is 1 new pair, so we divide 2520 by 4! to get that there are 105 distinct pairings.

(Note that $2520 = C_2^8 C_2^6 C_2^4 C_2^2 = (\frac{(8)(7)}{2})(\frac{(6)(5)}{2})(\frac{(4)(3)}{2})(\frac{(2)(1)}{2}) = \frac{8!}{2^4}$ and $105 = \frac{8!}{4!(2^4)} = \frac{(8)(7)(6)(5)}{2^4} = \frac{(2^3)(7)(2 \cdot 3)(5)(1)}{2^4} = (7)(5)(3)(1)$.)

To find the number of desired pairings (exactly 1 (B, G) pair), first consider that there are $\frac{C_2^5 C_2^3}{2!}$ ways to choose 2 (B, B) pairs from 5 boys. There are C_2^3 ways to choose 1 (G, G) pair from 3 girls. The remaining one boy and one girl has only one way to form a pair, so there are $\frac{C_2^5 C_2^3}{2!} \times C_2^3 = 45$ distinct desired pairings.

Thus P(exactly 1 pair of (B,G))= $\frac{45}{105} = \boxed{\frac{3}{7}}$

Discussion 62. For Solution a, the unsimplified probability is $\frac{P_2^5 P_2^3 P_2^3 4!}{8!}$, and for Solution b, the unsimplified probability is $\frac{\frac{C_2^5 C_2^3}{2!} C_2^3}{\frac{8!}{4!(2^4)}} = \frac{\frac{P_2^5 P_2^3 P_2^3 4!}{2^4}}{\frac{8!}{(2^4)}} = \frac{P_2^5 P_2^3 P_2^3 4!}{8!}$. Thus we can find only the number of distinct pairings for both the numerator and denominator of the probability to simplify the workings. Even though the unsimplified probability of Solution b seems more complicated, note that it can be written as

$$\frac{\frac{C_2^5 C_2^3}{2!} C_2^3}{\frac{8!}{4!(2^4)}} = \frac{(5)(3)(1)C_2^3}{(7)(5)(3)(1)} = \frac{3}{7}$$

The fact that the number of distinct pairings of 8 objects can be written in the form (7)(5)(3)(1) is not just a coincidence. In general, for even number $m = 2n$, we have:

Preposition (Pairing identity for even numbers)**.**

$$(2n-1)(2n-3)\cdots(3)(1) = \frac{(2n)!}{n!(2^n)}$$

Proof. When $n = 1$, RHS $= \frac{2!}{(1)(2)}$ = LHS .

$\therefore$ The statement is true for $n = 1$.

Assume that $(2k-1)(2k-3)\cdots(3)(1) = \dfrac{(2k)!}{k!(2^k)}$ for some k.

When $n = k+1$,

$$\begin{aligned}\text{LHS} &= (2k+1)(2k-1)(2k-3)\cdots(3)(1)\\ &= (2k+1)\frac{(2k)!}{k!(2^k)}\\ &= \frac{2(k+1)(2k+1)!}{2(k+1)k!(2^k)}\\ &= \frac{(2k+2)(2k+1)!}{2(k+1)k!(2^k)}\\ &= \frac{(2k+2)!}{(k+1)!(2^{k+1})}\\ &= \frac{(2(k+1))!}{(k+1)!(2^{k+1})}\\ &= \text{RHS}\end{aligned}$$

$\therefore$ The statement is true for $n = k+1$.

By mathematical induction, the statement is true for all positive integers n . □

For odd numbers $m = 2n+1$, we have:

Preposition (Pairing identity for odd numbers)**.**

$$(2n+1)(2n-1)(2n-3)\cdots(3)(1) = \frac{(2n+1)!}{n!(2^n)}$$

Proof. We have just proven that

$$(2n-1)(2n-3)\cdots(3)(1) = \frac{(2n)!}{n!(2^n)} \qquad \text{(pairing identity for even numbers)}$$

Multiply both sides by 2n+1 :

$$(2n+1)(2n-1)(2n-3)\cdots(3)(1) = \frac{(2n+1)!}{n!(2^n)}$$

□

So we have the pairing theorem:

Theorem 2.13. The number of distinct pairings (denoted as a_n) of n distinct objects is

$$a_n = \begin{cases} \dfrac{n!}{(\frac{n-1}{2})!(2^{\frac{n-1}{2}})} = (n)(n-2)\cdots(3)(1) & \text{if } n \text{ is odd} \\ \dfrac{n!}{(\frac{n}{2})!(2^{\frac{n}{2}})} = (n-1)(n-3)\cdots(3)(1) & \text{if } n \text{ is even} \end{cases}$$

Alternatively,

$$a_n = \frac{n!}{\lfloor\frac{n}{2}\rfloor!(2^{\lfloor\frac{n}{2}\rfloor})} = (2\lfloor\frac{n-1}{2}\rfloor + 1)(2\lfloor\frac{n-1}{2}\rfloor - 1)\cdots(3)(1)$$

Let's try a buffed version of the previous sub-problem.

Problem 62.2. In a class, there are 13 boys and 9 girls. The teacher randomly pairs up all the students. What is the probability that there are exactly 5 pairs of students which consist of one boy and one girl?

(Difficulty level: 7)

Solution 62.2. There are a total of $\dfrac{22!}{11!(2^{11})}$ possible distinct pairings.

For the distinct desired pairings, there must be exactly 5 (B, G) pairs, 4 (B, B) pairs and 2 (G, G) pairs. First we consider (B, B) pairs. There are $\dfrac{C_2^{13}C_2^{11}C_2^9C_2^7}{4!} = \dfrac{P_8^{13}}{4!(2^4)}$ ways to make 4 (B, B) pairs from 13 boys. Similarly, there are $\dfrac{C_2^9C_2^7}{2!} = \dfrac{P_4^9}{2!(2^2)}$ ways to make 2 (G, G) pairs from 4 girls.

The remaining 5 boys and 5 girls form 5 (B, G) pairs. Arbitrarily label the boys from 1 to 5. For the 1st boy, there are 5 girls to pair him with. For the 2nd boy, there are 4 remaining girls to pair him with, and so on, so there are 5! ways to form 5 (B, G) pairs.

Thus, P(exactly 5 (B, G) pairs)= $\dfrac{\dfrac{P_8^{13}P_4^9}{4!(2!)(2^4 2^2)}(5!)}{\dfrac{22!}{11!(2^{11})}} = \boxed{\dfrac{144}{323}}$

In general,

Theorem 2.14. When there are a object A and b object B, and the objects are paired randomly, then the probability of having exactly m distinct (A, B) pairs is (where $a+b$, $a-m$ and $b-m$ are even numbers):

$$\frac{P^a_{a-m}P^b_{b-m}(2^m)(\lfloor\frac{a+b}{2}\rfloor)!\,m!}{(a+b)!(\frac{a-m}{2})!(\frac{b-m}{2})!}$$

Problem 63. You are in possession of 25 pairs of socks (hence a total of 50 socks) ranging in shades of grey, with each pair labeled from 1 (white) to n (black). Take the socks blindly from a drawer and pair them at random. (This means randomly take two socks without replacement and make them a new pair. This process is then repeated until no socks are left.)

What is the probability that they are paired so that the colours of any pair differ by at most 1?

(In other words, find the probability that any manual pairing of two socks with label i and j have $|i-j| \leq 1$.)

(Difficulty level: 8) [17]

Solution 63.1. Let's start with some small examples. Let there be n pair of socks, and label each member of the i th pair as i_1 and i_2 . Let a_n be the number of pairings that satisfy the condition (with regard to the order within the same pair and the order that different pairs appear).

If $n = 1$, then the only possible pairing is $(1_1, 1_2)$ and $(1_2, 1_1)$, so $a_1 = 2$.

If $n = 2$, then we have the socks $\{1_1, 1_2, 2_1, 2_2\}$, so any pairing satisfies the condition, and there are 4! ways to pair the 4 socks (it is the same as 4-permutation), so $a_2 = 24$.

If $n = 3$, then first we can consider the pairings in which $(3, 3)$ is a pair, and there are two ways to order $(3, 3)$. The rest of the 4 socks $\{1_1, 1_2, 2_1, 2_2\}$ is just the socks available in a_2 , so we have $a_2 = 24$ ways to arrange these 4 socks. We can place the new pair $(3, 3)$ among the a_2 pairs in 3 ways, namely $(a, b), (c, d), (3, 3)$; $(a, b), (3, 3), (c, d)$; $(3, 3), (a, b), (c, d)$, so we have $2 \times 3 \times 24 = 144$ pairings so far.

Then we can consider the pairings that include $(3,2)$ and $(3,2)$ (in any order). There are 16 ways to have the pairing $(3,2),(3,2)$, namely

$(2_1,3_1),(2_2,3_2)$; $(2_2,3_1),(2_1,3_2)$; $(2_1,3_2),(2_2,3_1)$; $(2_2,3_2),(2_1,3_1)$;
$(3_1,2_1),(2_2,3_2)$; $(3_2,2_1),(2_1,3_2)$; $(3_1,2_2),(2_2,3_1)$; $(3_2,2_2),(2_1,3_1)$;
$(2_1,3_1),(3_2,2_2)$; $(2_2,3_1),(3_1,2_2)$; $(2_1,3_2),(3_2,2_1)$; $(2_2,3_2),(3_1,2_1)$;
$(3_1,2_1),(3_2,2_2)$; $(3_2,2_1),(3_1,2_2)$; $(3_1,2_2),(3_2,2_1)$; $(3_2,2_2),(3_1,2_1)$.

The remaining socks $(1,1)$ can be arranged in $a_1 = 2$ ways, and we can place these two new pairings among $(1,1)$ in C_2^3 ways, so we have $2 \times C_2^3 \times 16 = 96$ for the $(3,2)$ pairings.

In total, we have $144 + 96 = 240$ pairings, so $a_3 = 240$.

By similar reasoning, we have $a_4 = (2)(4)a_3 + (C_2^4)(16)a_2 = 4224$

And in general, we have the recursive formula

$$\begin{aligned} a_n &= 2n\, a_{n-1} + 16\, C_2^n\, a_{n-2} \\ &= 2n\, a_{n-1} + 16\, (\frac{n(n-1)}{2})\, a_{n-2} \\ &= 2n\, a_{n-1} + 8n(n-1)\, a_{n-2} \end{aligned}$$

with the initial condition $a_1 = 2$, $a_2 = 24$.

Let p_n be the probability the pairings satisfy the condition. The number of possible outcomes for n pairs of socks is $2n!$, so $p_n = \dfrac{a_n}{(2n)!}$

Using python to find a_{25}:

```
def a(n):
    res = [1,2] + [0] * (n-1)
    for i in range(2,n+1):
        res[i] += 2 * i * res[i-1] + 8 * i * (i-1) * res[i-2]
    return res[-1]
print(a(25))
```

And we get

```
11642713121711873052994223260827648000000
```

So $P(\text{colours differ by at most 1})$

$$= \frac{a_{25}}{(2 \cdot 25)!}$$

$$= \frac{116427131217118730529942232608276480000000}{30414093201713378043612608166064768844377641568960512000000000000}$$

$$= \boxed{\frac{22369621}{584358414459472720534554743906 25}}$$

Discussion 63.1. The general formula of a_n is

$$a_n = \frac{(2^{n+1} + (-1)^n)2^n n!}{3}$$

The fastest way to prove it is to use mathematical induction:

Let a_n be a sequence defined by the recursive formula $a_n = 2n\, a_{n-1} + 8n(n-1)a_{n-2}$ with the initial condition $a_1 = 2$, $a_2 = 24$. We need to show that the formula

$$a_n = \frac{(2^{n+1} + (-1)^n)2^n n!}{3}$$

is true for all positive integers n .

When $n = 1$, RHS $= \frac{(2^2+(-1))2(1)}{3} = 2 =$ LHS

When $n = 2$, RHS $= \frac{(2^3+1)2^2(2)}{3} = 24 =$ LHS

$\therefore$ The formula is true for $n = 1$ and $n = 2$.

Assume that the formula is true $n = k$ and $n = k + 1$. We have

$$a_k = \frac{(2^{k+1} + (-1)^k)2^k k!}{3} \quad \text{and} \quad a_{k+1} = \frac{(2^{k+2} + (-1)^{k+1})2^{k+1}(k+1)!}{3}$$

When $n = k + 2$,

$$\begin{aligned}
\text{LHS} &= a_{k+2} \\
&= 2(k+2)\, a_{k+1} + 8(k+2)(k+1)a_k \qquad\qquad \text{(recursive formula with } n = k+2) \\
&= 2(k+2)(\frac{(2^{k+2} + (-1)^{k+1})2^{k+1}(k+1)!}{3}) + 8(k+2)(k+1)(\frac{(2^{k+1} + (-1)^k)2^k k!}{3}) \\
&= \frac{k+2}{3}\left(2(2^{k+2} + (-1)^{k+1})2^{k+1}(k+1)! + 2^3(2^{k+1} + (-1)^k)2^k(k+1)!\right) \\
&= \frac{(k+1)!(k+2)}{3}\left((2^{k+2} + (-1)^{k+1})2^{k+2} + (2^{k+1} + (-1)^k)2^{k+3}\right) \\
&= \frac{2^{k+2}(k+2)!}{3}\left((2^{k+2} + (-1)^{k+1}) + (2^{k+1} + (-1)^k)2\right) \\
&= \frac{2^{k+2}(k+2)!}{3}\left(2^{k+2} + (-1)^{k+1} + 2^{k+2} + 2(-1)^k\right) \\
&= \frac{2^{k+2}(k+2)!}{3}\left(2(2^{k+2}) + (-1)^k(-1+2)\right) \\
&= \frac{\left(2^{k+1+2} + (-1)^{k+2}\right) 2^{k+2}(k+2)!}{3} \\
&= \text{RHS}
\end{aligned}$$

The formula is true for $n = k + 2$.

$\therefore$ By mathematical induction, the formula is true for all positive integers n .

Solution 63.2. Note that we counted the order within the same pair and the order that different pairs appear in both the numerator and denominator of the probability. We can actually only count the distinct pairings. The number of possible distinct manual pairings of n pairs of socks is $\dfrac{(2n)!}{n!(2^n)}$. Let b_n denote the number of distinct desired pairings.

If $n = 1$, then the only possible pairing is $(1, 1)$, so $b_1 = 1$.

If $n = 2$, then we have the socks $\{1, 1, 2, 2\}$, so any pairing satisfies the condition, and there are $(3)(1) = 3$ ways to pair the 4 socks, so $b_2 = 3$.

If $n = 3$, then first we can consider the pairings in which $(3, 3)$ is a pair. The rest of the 4 socks $\{1_1, 1_2, 2_1, 2_2\}$ is just the socks available in a_2 , so we have $a_2 = 3$ pairings so far.

Then we can consider the pairings that include $(3, 2)$ and $(3, 2)$. There are two ways to pair '3' and '2' , namely $(3_1, 2_1), (3_2, 2_2)$ and $(3_2, 2_1), (3_1, 2_2)$

. The remaining socks $(1,1)$ can be arranged in $a_1 = 1$ ways, so we have $2 \times b_1$ for the $(3,2)$ pairings.

In total, we have $b_2 + 2b_1 = 5$ pairings, so $b_3 = 5$.

By similar reasoning, we have $b_4 = b_3 + 2b_2 = 11$ pairings, and in general:

$$b_n = b_{n-1} + 2b_{n-2}$$

with initial conditon $b_1 = 1$, $b_2 = 3$. (We can also use $b_0 = 1$.)

Using python to find b_{25}:

```
def b(n):
    res = [1,1] + [0] * (n-1)
    for i in range(2, n+1):
        res[i] = res[i-1] + 2 * res[i-2]
    return res[-1]
print(b(25))
```

And we get

```
    22369621
```

So $P(\text{colours differ by at most 1})$

$$= \frac{22369621}{\frac{50!}{25!(2^{25})}}$$

$$= \boxed{\frac{22369621}{58435841445947272053455474390625}}$$

2.8.3 Solving for linear recursive formulas

Discussion 63.1. Notice that $\frac{a_n}{b_n} = n!(2^n)$. We can use induction to verify this:

$$\frac{a_1}{b_1} = \frac{2}{1} = 1!(2^1) \quad \text{and} \quad \frac{a_2}{b_2} = \frac{24}{3} = 2!(2^2)$$

Assume that $\dfrac{a_{k-1}}{b_{k-1}} = (k-1)!(2^{k-1})$ and $\dfrac{a_{k-2}}{b_{k-2}} = (k-2)!(2^{k-2})$ for some k .

$$\begin{aligned}
\frac{a_k}{b_k} &= \frac{2k\,a_{k-1} + 8k(k-1)a_{k-2}}{b_{k-1} + 2b_{k-2}} \\
&= \frac{2k\,(k-1)!(2^{k-1})b_{k-1} + 2^3k(k-1)(k-2)!(2^{k-2})b_{k-2}}{b_{k-1} + 2b_{k-2}} \\
&= \frac{k!(2^k)b_{k-1} + k!(2^{k+1})b_{k-2}}{b_{k-1} + 2b_{k-2}} \\
&= \frac{k!(2^k)(b_{k-1} + 2b_{k-2})}{b_{k-1} + 2b_{k-2}} \\
&= k!(2^k)
\end{aligned}$$

$\therefore \dfrac{a_n}{b_n} = n!(2^n)$ for all positive integers n .

The recursive formula of b_n is a lot simpler, so it is much easier to find its general formula:

Let's start with an even simpler recursive formula: $c_n = 2c_{n-1}$ with $c_0 = 1$. Then we can easily see that $c_n = 2^n$. Maybe the general formula of b_n will follow a similar pattern.

Let's guess that for some r , $b_n = r^n$ is true for all $n \in \mathbb{Z}^+$. Starting with the recursive formula of b_n:

$$b_n = b_{n-1} + 2b_{n-2}$$

$$r^n = r^{n-1} + 2r^{n-2}$$

Cancel r^n on both sides and multiply by r^2:

$$r^2 = r + 2$$

$$r^2 - r - 2 = 0$$

$$r = 2 \quad \text{or} \quad r = -1$$

This suggests that $b_n = 2^n$ or $b_n = (-1)^n$. That's not quite right, since b_n is obviously not a sequence of powers of 2 or powers of -1. So why do we bother doing this? As it turns out, we have just found out two general formulas that also satisfies the recursive formula $b_n = b_{n-1} + 2b_{n-2}$, although with different starting values .

Let α_n be the n th term of the sequence that uses $r = 2$, and let β_n be the n th term of the sequence that uses $r = -1$. We have $\alpha_n = 2^n$ with $\alpha_0 = 1$, $\alpha_1 = 2$, and $\beta_n = (-1)^n$ with $\beta_0 = 1$, $\beta_1 = -1$.

As α_n and β_n satisfy the recursive formula $b_n = b_{n-1} + 2b_{n-2}$, we have (for all $n \geq 2$):

$$\alpha_n - \alpha_{n-1} - 2\alpha_{n-2} = 0 \quad \text{and} \quad \beta_n - \beta_{n-1} - 2\beta_{n-2} = 0 \qquad \ldots(*)$$

Let $d_n = A\alpha_n + B\beta_n$ for some A, B . Then for all $n \geq 2$:

$$\begin{aligned} d_n &= A\alpha_n + B\beta_n && (1) \\ d_{n-1} &= A\alpha_{n-1} + B\beta_{n-1} && (2) \\ 2d_{n-2} &= 2A\alpha_{n-2} + 2B\beta_{n-2} && (3) \end{aligned}$$

(1) – (2) – (3) :

$$\begin{aligned} d_n - d_{n-1} - 2d_{n-2} &= A(\alpha_n - \alpha_{n-1} - 2\alpha_{n-2}) + B(\beta_n - \beta_{n-1} - 2\beta_{n-2}) \\ &= 0 \qquad\qquad\qquad\qquad \text{(by (*))} \\ d_n &= d_{n-1} + 2d_{n-2} \end{aligned}$$

Thus, no matter what values A and B are, d_n must also satisfy the recursive formula $b_n = b_{n-1} + 2b_{n-2}$. Now what if we set $b_n = d_n$ with some specific value of A, B such that $b_1 = 1$ and $b_2 = 3$? This way, $b_3 = (3) + 2(1) = 5$ and so on and we will get our familiar b_n sequence. Hopefully it will work. (equation counter reset)

$$b_n = A\alpha_n + B\beta_n$$

$$\begin{cases} b_1 = A\alpha_1 + B\beta_1 = 1 & \ldots(1) \\ b_2 = A\alpha_2 + B\beta_2 = 3 & \ldots(2) \end{cases}$$

Substitute $\alpha_n = 2^n$ and $\beta_n = (-1)^n$:

$$\begin{cases} A(2^1) + B(-1)^1 = 1 & \ldots(1) \\ A(2^2) + B(-1)^2 = 3 & \ldots(2) \end{cases}$$

$$\begin{cases} 2A - B = 1 & \ldots(1) \\ 4A + B = 3 & \ldots(2) \end{cases}$$

Solving, we get $A = \dfrac{2}{3}$, $B = \dfrac{1}{3}$.

So $b_n = \frac{2}{3}(2^n) + \frac{1}{3}(-1)^n = \frac{2^{n+1} + (-1)^n}{3}$. It works. This way, we can derive the very-hard-to-derive general formula above in [Discussion 1] by using the fact that $a_n = n!(2^n)b_n$:

$$a_n = \frac{(2^{n+1} + (-1)^n)2^n n!}{3}$$

2.9 Elementary number theory

When we are counting stuff, sometimes it involves the properties of integers. For example, we may need to count the number of ways that the sum of n integers between 1 and 100 inclusive is divisible by k. How do we solve these kind of problems? This is why we take a look at **Number theory**, which is the study of integers and their properties.

2.9.1 Properties of divisibility

First, let me introduce some notations.

Notations (the bullet points are not a part of notation)

- $a \Dashv b$ means the statement "a divides b" / "a is a divisor (factor) of b" / " b is a multiple of a"

  (Mathematically, let a, b be integers. Then $a \Dashv b$ if and only if there exists an integer k such that $b = ka$.)

  (This notation differs from the conventional notation '$a \,|\, b$' as $|$ is reserved for 'given' or 'such that' in this article. Plus, I think using $|$ to mean 'divides' is stupid.)

- $a \nmid b$ means the statement "a does not divide b" / "a is not a divisor (factor) of b" / " b is not a multiple of a"

  (Mathematically, let a, b be integers. Then $a \nmid b$ if and only if there does not exist an integer k such that $b = ka$.)

  (This is the conventional 'does not divide' notation.)

- $\gcd(a, b)$ means the greatest common divisor (/ highest common factor) of a and b

  (Mathematically, $\gcd(a, b)$ is the greatest positive integer c that satisfies both $c \Dashv a$ and $c \Dashv b$ for a, b not both $= 0$.)

- $\operatorname{lcm}(a, b)$ means the least common multiple of a and b

  (Mathematically, $\operatorname{lcm}(a, b)$ is the least positive integer c that satisfies both $a \Dashv c$ and $b \Dashv c$ for $a, b \neq 0$.)

- $a \models b$ means the statement "a can be (evenly) divided by b" / "b is a divisor (factor) of a" / " a is a multiple of b"

  (Nobody uses this notation.)

- $\mathbb{Z}^{\backslash 0}$ means the set of all integers except 0 (or $\mathbb{Z}\backslash\{0\}$)

- $\mathbb{N}$ means the set of all natural numbers (which includes 0) / the set of all non-negative integers

- $\mathbb{Z}^{+}$ means the set of all positive integers

- $\{A \,|\, B\}$ and $\{A : B\}$ mean the set of all stuff that satisfies statement A given that it satisfies statement B / the set of all stuff that satisfies statement A such that it satisfies statement B .

  (This is called the set builder notation. For example, $\{x^2 \,|\, x \in \mathbb{N}\}$ is the set of all integers that is a square number. The two notations above are equivalent, and can be used interchangeably.)

Division algorithm [18]

Before I dive into the divisibility stuff, let's first talk about the **division algorithm**. It states that for all a, $b \in \mathbb{Z}$ with $b > 0$, there exists unique integers q, $r \in \mathbb{Z}$ such that

$$a = bq + r \qquad \text{with } 0 \leq r < b$$

. This means that every integer can be written in the form of divisor × quotient + remainder .

Proof. Consider the set $S = \{a - bx \,|\, x \in \mathbb{Z}, a - bx \geq 0\}$. This is the set of all $a - bx$ with non-negative value (a, b are fixed while x is variable when constructing this set).

No matter what a, b are given initially, this set will always have at least one element (i.e. S is not an empty set) . This is because if $a \geq 0$, we can choose $x = 0$ so that $a - b(0) = a \geq 0$ is one of the elements of S . If $a < 0$, we can choose $x = a$ so that $a - b(a) = a(1 - b) \geq 0$ is one of the elements of S. Note: $a(1 - b) \geq 0$ is true since $a < 0$ and $1 - b \leq 0$ (b must be at least 1 from the parameters given).

Since S has at least one element and has a lower bound of 0, the minimum element always exists.

Let r be the minimum element of S , and q be the corresponding x-value (so $q = \frac{a-r}{b}$.) Then $r = a - bq$ and $a = bq + r$. We need to show that $0 \leq r < b$. Obviously, $r \geq 0$ since r is an element of S.

Let's show $r < b$ by contradiction. Suppose that $r \geq b$. Then we have

$$r = a - bq \geq b$$

Subtract b for both sides of equation: $r - b = a - b(q+1) \geq 0$

$r - b$ is in the form of $a - bx$, so it is an element of S. We found an element $r - b$ that is smaller than the supposedly minimum element r, which is a contradiction. So $r < b$ must be true.

Now we prove the uniqueness of q and r. Suppose that $a = bq+r = bq'+r'$. We have $b(q - q') = r' - r$. In the LHS, we see that $q - q'$ is a multiple of b, and in the RHS, we see that $0 \leq r' - r < b$ (since both r and r' are between 0 and $b - 1$ inclusive). Since $r' - r$ is less than b itself, the only possibility is that $q - q' = r' - r = 0$. Thus, we conclude that $q = q'$ and $r = r'$.

□

The division algorithm can be extended to when b is negative. We have $a = |b|\, q + r$. If $b < 0$, then $-b = |b|$ and we have:

$$\begin{aligned} & a = (-b)q + r \\ & a = b(-q) + r \\ \text{Let } p = -q : \quad & a = bp + r \end{aligned}$$

There is still a unique representation of a in the form $a = bp + r$.

Properties of divisibility, lcm and gcd, primes and coprimes

(The variables mentioned are assumed to be positive integers unless stated otherwise. If there is $(\forall a \in \mathbb{Z})$ or the like beside the statement, then the variables mentioned in the statement or the proof can be any integers.)

Here are some basic properties of the 'divides' relation.

1. $a \Dashv a \quad (\forall a \in \mathbb{Z})$ (reflexive property)

Proof. $a = 1a \;\Rightarrow\; a \Dashv a$ □

2. $1 \Dashv a \quad (\forall a \in \mathbb{Z})$ (1 is a divisor of all integers)

Proof. $a = (a)(1) \;\Rightarrow\; 1 \Dashv a$ $\square$

3. $a \Dashv 0 \quad (\forall a \in \mathbb{Z})$ (all integers are divisors of 0)

Proof. $0 = 0a \;\Rightarrow\; a \Dashv 0$ $\square$

4. $0 \nmid a \quad (\forall a \in \mathbb{Z}^{\setminus 0})$ (0 can't divide other integers)

Proof. If $a \neq 0$, then $a \neq 0k$ for all $k \;\Rightarrow\; 0 \nmid a$. $\square$

5. $a \Dashv b \;\Leftrightarrow\; a \Dashv -b \;\Leftrightarrow\; -a \Dashv b \;\Leftrightarrow\; -a \Dashv -b \quad (\forall a, b \in \mathbb{Z})$
(negation property)

Proof. $a \Dashv b \;\Leftrightarrow\; b = ka \;\Leftrightarrow$ for some $k \in \mathbb{Z} \;\Leftrightarrow\; (-b) = (-k)a$
$\Leftrightarrow\; b = (-k)(-a) \;\Leftrightarrow\; (-b) = k(-a)$ $\square$

6. If $a \Dashv b$, then $a \leq b$ (a number's divisor can't be larger than itself)

Proof. $a \Dashv b \;\Rightarrow\; b = ka$ for some $k \geq 1 \;\Rightarrow\; k = \frac{b}{a} \geq 1$
$\Rightarrow\; b \geq a \;\Rightarrow\; a \leq b$ $\square$

6.5. If $a > b$, then $a \nmid b$ (contraposition of (6))

7. Iff $a \Dashv b$ and $b \Dashv a$, then $a = b$ (symmetry implies equality)

Proof. $(\Rightarrow)\;\; a \Dashv b \;\Rightarrow\; a \leq b \;\; ; \;\; b \Dashv a \;\Rightarrow\; b \leq a \;\Rightarrow\; a = b$
$(\Leftarrow)\;\; a = b \;\Rightarrow\; a \Dashv b$ and $b \Dashv a$ (reflexive property) $\square$

8. If $a \Dashv b$ and $b \Dashv c$, then $a \Dashv c \quad (\forall a, b, c \in \mathbb{Z})$ (transitive property)

Proof. Let $b = ka$ and $c = lb$. Then $c = lb = l(ka) = (lk)a$
$\Rightarrow\; a \Dashv c$ $\square$

9. Iff $a \Dashv b$, then $ka \Dashv kb \quad (\forall a, b \in \mathbb{Z}, k \in \mathbb{Z}^{\setminus 0})$ (scaling property)

Proof. $b = ma. \;\Leftrightarrow\; kb = m(ka) \;\Leftrightarrow\; ka \Dashv kb$ $\square$

10. $a \Dashv ak \quad (\forall a, k \in \mathbb{Z})$ (a number divides its multiple)

Proof. $1 \Dashv k$ (1 is a divisor of all integers) $\Rightarrow$ $a \Dashv ak$ (scaling property) □

11. If $a \Dashv b$, then $a \Dashv kb \quad (\forall a, b, k \in \mathbb{Z})$ (divisor divides number's multiple)

Proof. We have $b \Dashv kb$ (a number divides its multiple). If $a \Dashv b$, then $a \Dashv kb$ by transitive property. □

12. If $c \Dashv a$ or $c \Dashv b$, then $c \Dashv ab \quad (\forall a, b, c \in \mathbb{Z})$
(property of divisibility sharing)

Proof. If $c \Dashv a$, then $a = kc \;\Rightarrow\; ab = (kc)b = (kb)c \;\Rightarrow\; c \Dashv ab$

Similarly, if $c \Dashv b$, then $b = lc \;\Rightarrow\; ab = a(lc) = (al)c \;\Rightarrow\; c \Dashv ab$ □

Note: The converse is true only if c is a prime (see Euclid's lemma).

13. If $a \Dashv b$ and $c \Dashv d$, then $ac \Dashv bd$. $(\forall a, b, c, d \in \mathbb{Z})$ (multiplicative property)

Proof. Let $b = ka$ and $d = lc$. Then $bd = (ka)(lc) = (kl)ac$

$\Rightarrow \; ac \Dashv bd$ □

14. If $c \Dashv a$ and $c \Dashv (a + b)$, then $c \Dashv b \quad (\forall a, b, c \in \mathbb{Z})$
(property of divisible sum) [19]

Proof. Let $a = kc$ and $a + b = lc$. Then

$\Rightarrow \; b = lc - a = lc - kc = (l - k)c \;\Rightarrow\; c \Dashv b$ □

15. If $a \nmid b$, then $a \nmid b + ka \quad (\forall a, b, k \in \mathbb{Z})$ (property of indivisible steps)

Proof. We prove the contrapositive of the statement, which is equivalent to the original statement.

If $a \Dashv b + ka$, then since we also have $a \Dashv ka$ (a number divides its multiple), it follows that $a \Dashv b$ (property of divisible sum). □

16. If $c \Dashv a$ and $c \Dashv b$, then $c \Dashv (ax+by) \quad (\forall a,b,c,x,y \in \mathbb{Z})$
(property of linear combination) [19]

Proof. Let $a = kc$ and $b = lc$. Then $ax + by = (kc)x + (lc)y$
$= (kx + ly)c \;\Rightarrow\; c \Dashv (ax + by)$ □

17. Let a, b be non-zero integers. Then there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. (Bézout's identity) [20]

Proof. Given any non-zero integers a and b, let
$S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$ be the set of all positive linear combinations of a, b. The set S is non-empty since we can make a positive element by choosing some specific values of x and y based on different conditions:

$$\begin{aligned}
a > 0 \;\Rightarrow&\qquad |a| = 1{\times}a + 0{\times}b \\
a < 0 \;\Rightarrow&\qquad |a| = (-1){\times}a + 0{\times}b \\
b > 0 \;\Rightarrow&\qquad |b| = 0{\times}a + 1{\times}b \\
b < 0 \;\Rightarrow&\qquad |b| = 0{\times}a + (-1){\times}b
\end{aligned}$$

Since S is non-empty and has a lower bound of 0, it has a minimum element $d = as + bt$ for some $s, t \in \mathbb{Z}$.

To prove that d is the greatest common divisor of a and b, it must be proven that d is a common divisor of a and b, and that for any other common divisor c, one has $c \leq d$.

By the division algorithm, there exists $q, r \in \mathbb{Z}$ with $a = dq + r$ with $0 \leq r < d$. Then $r = a - qd = a - q(as + bt) = a(1 - qs) - bqt$.

Thus r is in the form $ax+by$ (linear combination of a and b), and hence $r \in S \cup \{0\}$. However, $0 \leq r < d$, and d is the smallest positive integer in S. The remainder r can therefore not be in S, making r necessarily 0. This means $a = dq$, and d is a divisor of a.

Similarly, if we repeat the argument for b, we have $b = dq + r$
$\Rightarrow\; r = b - qd = b - q(as + bt) = b(1 - qt) - aqs$. By similar reasoning, d is also a divisor of b, and therefore d is a common divisor of a and b.

Now, let c be any common divisor of a and b; that is, there exist $u, v \in \mathbb{Z}$ such that $a = cu$ and $b = cv$. Thus

$$d = as + bt = cus + cvt = c(us + vt)$$

That is, c is a divisor of d. Since $d > 0$, this implies $c \leq d$.

Therefore, $d = \gcd(a, b)$. □

18. Iff $c \Dashv a$ and $c \Dashv b$, then $c \Dashv \gcd(a,b)$ (GCD universal property)

Proof. ($\Rightarrow$) By Bézout's identity, there exists $x,\ y \in \mathbb{Z}$ such that $ax + by = \gcd(a,b)$.

If $c \Dashv a$ and $c \Dashv b$, then $c \Dashv (ax+by)$ by property of linear combination.
$\Rightarrow\ c \Dashv \gcd(a,b)$

($\Leftarrow$) Now we proof the converse. By definition, $\gcd(a,b) \Dashv a$ and $\gcd(a,b) \Dashv b$.

If $c \Dashv \gcd(a,b)$, then $c \Dashv a$ by transitive property of divisibility. Similarly, if $c \Dashv \gcd(a,b)$, then $c \Dashv b$ by transitive property. □

19. $\gcd(ka,kb) = k \cdot \gcd(a,b)$ (GCD distributive property)

Proof. [21] Let $d = \gcd(a,b)$ and $w = \gcd(ka,kb)$. Then by definition of GCD, we have

$d \Dashv a$ and $d \Dashv b \Rightarrow kd \Dashv ka$ and $kd \Dashv kb$ (scaling property)

$\Rightarrow\ kd \Dashv \gcd(ka,kb)$ (GCD universal property) $\Rightarrow\ kd \Dashv w$

$\Rightarrow\ w = kdx$ for some $x > 0$.

By definition of GCD, we have $w \Dashv ka$ and $w \Dashv kb$. Substitute $w = kdx$,

$\Rightarrow\ kdx \Dashv ka$ and $kdx \Dashv kb$

$\Rightarrow\ dx \Dashv a$ and $dx \Dashv b$ (scaling property)

$\Rightarrow\ dx \Dashv \gcd(a,b)$ (GCD universal property) $\Rightarrow\ dx \Dashv d$

$\Rightarrow\ x \Dashv 1$ (scaling property) $\Rightarrow\ 1 = mx$ for some $m > 0$.

Since $x > 0$ and $m > 0$, it must be that $x = m = 1$.

Thus, $\gcd(ka,kb) = w = kd(1) = k \cdot \gcd(a,b)$. □

20. $\operatorname{lcm}(a,b) \cdot \gcd(a,b) = ab$ (property of product of LCM and GCD)

Proof. [22] Let $d = \gcd(a,b)$. By definition of GCD, $d \Dashv a$ and $d \Dashv b$

$\Rightarrow\ d \Dashv ab$ (multiplicative property)

$\Rightarrow\ \exists$ (there exists) n such that $ab = dn$. $\ldots(*)$

We have $d \Dashv a$ and $d \Dashv b$.

$$\begin{aligned}
&\Rightarrow \ \exists u, v : & a = du \ \text{ and } \ b = dv & \\
&\Rightarrow & dub = dn \ \text{ and } \ adv = dn & \qquad \text{by (*)} \\
&\Rightarrow & bu = n \ \text{ and } \ av = n & \\
&\Rightarrow & a \Dashv n \ \text{ and } \ b \Dashv n &
\end{aligned}$$

Let m be a common multiple of a, b. We have $a \Dashv m$ and $b \Dashv m$. Then $m = ar = bs$ for some r, s .

Also, by Bézout's Identity we have $d = ax + by$ for some $x, y \in \mathbb{Z}$.

So

$$\begin{aligned}
md &= axm + bym \\
&= ax(bs) + by(ar) \\
&= ab(sx + ry) \\
&= dn(sx + ry) && \text{by (*)} \\
m &= n(sx + ry)
\end{aligned}$$

Thus, $n \Dashv m \ \Rightarrow \ n \leq m$ (a number's divisor can't be larger than itself)

Since n is equal to or smaller than all common multiples of a, b, we conclude that n is the least common multiple of a, b . Thus $n = \operatorname{lcm}(a, b)$.

Therefore, $ab = dn = \operatorname{lcm}(a, b) \cdot \gcd(a, b)$. □

21. Iff $a \Dashv c$ and $b \Dashv c$, then $\operatorname{lcm}(a, b) \Dashv c$ (LCM universal property)

Proof. [23] ($\Rightarrow$) If $a \Dashv c$ and $b \Dashv c$, then we can let $c = ka = lb$. By Bézout's identity, there exists x, $y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. We have

$$c \cdot \gcd(a, b) = cax + cby = (lb)ax + (ka)by = ab(lx + ky)$$

Since $ab = \operatorname{lcm}(a, b) \cdot \gcd(a, b)$ by the property of product of LCM and GCD, we have

$$c \cdot \gcd(a, b) = \operatorname{lcm}(a, b) \cdot \gcd(a, b) \cdot (lx + ky)$$

$$c = \operatorname{lcm}(a, b) \cdot (lx + ky)$$

Thus, $\operatorname{lcm}(a, b) \Dashv c$.

($\Leftarrow$) Now we prove the converse. By definition, $a \Dashv \operatorname{lcm}(a,b)$ and $b \Dashv \operatorname{lcm}(a,b)$.

If $\operatorname{lcm}(a,b) \Dashv c$, then $a \Dashv c$ by transitive property of divisibility. Similarly, if $\operatorname{lcm}(a,b) \Dashv c$, then $b \Dashv c$ by transitive property. □

22. $\operatorname{lcm}(ka,kb) = k \cdot \operatorname{lcm}(a,b)$ (LCM distributive property)

Proof. [24] By the property of product of LCM and GCD,

$$\operatorname{lcm}(ka,kb) \cdot \gcd(ka,kb) = (ka)(kb) \tag{1}$$

Also, we have

$$\begin{aligned} \operatorname{lcm}(a,b) \cdot \gcd(a,b) &= ab \\ k\operatorname{lcm}(a,b) \cdot k\gcd(a,b) &= (ka)(kb) && \text{(multiply both sides by } k^2\text{)} \\ k\operatorname{lcm}(a,b) \cdot \gcd(ka,kb) &= (ka)(kb) && \text{(GCD distributive property)} \end{aligned} \tag{2}$$

Combine equation (1) and (2):

$$\begin{aligned} \operatorname{lcm}(ka,kb) \cdot \gcd(ka,kb) &= k\operatorname{lcm}(a,b) \cdot \gcd(ka,kb) \\ \operatorname{lcm}(ka,kb) &= k\operatorname{lcm}(a,b) \end{aligned}$$

□

23. $\gcd(a,ka) = a$ (GCD property of multiples)

Proof. Let $d = \gcd(a,ka)$. Then $d \Dashv a$ and $d \Dashv ka$. Also, we have $a \Dashv a$ (reflexive property) and $a \Dashv ka$ (a number divides its multiple). Since $d \leq a$ (a number's divisor can't be larger than itself), and d should be as large as possible, it must be that $d = a$. □

24. Iff $d = \gcd(a,b)$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ (GCD division property)

Proof. ($\Rightarrow$) Let $d = \gcd(a,b)$. Let $a = md$ and $b = nd$. If some $k > 1$ divides m and n, then $m = sk$ and $n = tk$ for some s, t .

Then $a = skd$ and $b = tkd$. We have $kd \Dashv a$ and $kd \Dashv b$, contradicting the fact that d is the greatest common divisor of a and b. Thus k must be 1, and $\gcd(m,n) = \gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

$(\Leftarrow)$ Let $m = \dfrac{a}{d}$ and $n = \dfrac{b}{d}$. Then $dm = a$ and $dn = b$.

$\gcd(m, n) = 1 \;\Rightarrow\; \gcd(dm, dn) = d \cdot \gcd(m, n)$ (GCD distributive property) $= d(1) \;\Rightarrow\; \gcd(a, b) = d$ □

25. Iff $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$

(property of coprime sharing)

Proof. $(\Rightarrow)$ By Bézout's Identity, there exists $x, y, z, w \in \mathbb{Z}$ such that $ax + by = 1$ and $az + cw = 1$, so

$$\begin{aligned} (ax + by)(az + cw) &= 1 \\ a^2xz + axcw + byaz + bycw &= 1 \\ a(axz + xcw + byz) + bc(yw) &= 1 \\ \gcd(a, bc) &= 1 \qquad \text{(Bézout's Identity)} \end{aligned}$$

$(\Leftarrow)$ Suppose $\gcd(a, bc) = 1$. Let $d = \gcd(a, b)$. Then $d \Dashv a$ and $d \Dashv b$, thus $d \Dashv a$ and $d \Dashv bc$ (divisor divides number's multiple) . Since d is a common divisor of a and bc , $d \leq \gcd(a, bc)$. But $\gcd(a, bc) = 1$ by assumption, which means $d = 1$ must be the case. By similar reasoning, we have $\gcd(a, c) = 1$ (seen by replacing b with c and vice versa in the argument). □

26. If $\gcd(a, b) = 1$, then $\gcd(a + bk, b) = 1 \quad (\forall k \in \mathbb{Z})$

(property of coprime steps)

Proof. By Bézout's Identity, $ax + by = 1$ for some $x, y \in \mathbb{Z}$.

Let $d = y - xk$ for $k \in \mathbb{Z} \;\Rightarrow\; y = d + xk$

$\Rightarrow\; ax + by = ax + b(d + xk) = ax + bd + bxk = (a + bk)x + (b)d = 1$

$\Rightarrow\; \gcd(a + bk, b) = 1$

□

27. For $a > 1$ and $b > 1$, if a and b are coprime, then $a \nmid b$ and $b \nmid a$

(property of coprimes)

Proof. We will prove the contrapositive statement.

If $a \Dashv b$ or $b \Dashv a$, then $b = ka$ or $a = mb$

$\Rightarrow$ $\gcd(a, b) = \gcd(a, ka) = a > 1$ or $\gcd(a, b) = \gcd(mb, b) = b > 1$ (GCD property of multiples)

$\Rightarrow$ a and b are not coprime. □

28. If $p > 1$ is not a prime (/is composite), then $p = ab$ for some a, b such that $1 < a, b < p$ (property of composite)

Proof. If $p > 1$ is not a prime, then there exists $a > 0$ such that $a \neq 1, p$ and $a \Dashv p$. Since $a \Dashv p$, we have $a \leq p$ because a number's divisor can't be larger than itself. Thus $1 < a < p$. Similarly, we have $1 < b < p$. □

29. If a, b are coprime and $a \Dashv bc$, then $a \Dashv c$

(property of divisibility inheritance)

Proof. ([25] p.10) Since $\gcd(a, b) = 1$, by Bezout's identity there are coefficients $x, y \in \mathbb{Z}$ such that $1 = ax + by$. Multiply both sides by c to get $c = cax + cby = a(cx) + (bc)y$. Note that $a \Dashv a$ and that $a \Dashv bc$ by assumption, so a divides the linear combination $a(cx) + (bc)y = c$ by the property of linear combination. Therefore $a \Dashv c$. □

30. If a, b are coprime with $a \Dashv c$ and $b \Dashv c$, then $ab \Dashv c$

(property of divisor product)

Proof. Since $\gcd(a, b) = 1$, by Bezout's identity there are coefficients $x, y \in \mathbb{Z}$ such that $1 = ax + by$.

Let $c = ka$ and $c = lb$. Then $c = cax + cby = (lb)ax + (ka)by$
$= ab(lx + ky)$ $\Rightarrow$ $ab \Dashv c$ □

31. If p is a prime, then $p \nmid a \iff p$ and a are coprime.

(property of prime)

Note: The meaning of the equivalence is that if one of the statement after 'then' is true, then the other statement after 'then' must also be true.

Proof. Assume that p is a prime. In the equivalence statement, we want to show that LHS $\Rightarrow$ RHS and LHS $\Leftarrow$ RHS.

($\Rightarrow$) Let $d = \gcd(p, a)$. Note that $d \Dashv p$ and $d \Dashv a$.

If p is a prime and $p \nmid a$, then since $d \Dashv p$ we have that $d = 1$ or $d = p$ by the definition of a prime. If $d = p$ then $p \Dashv a$, which we assumed was not true. So we must have $d = 1$. Hence $\gcd(p, a) = 1$.

($\Leftarrow$) Assume that $\gcd(p, a) = 1$. Then whenever $d \Dashv p$ and $d \Dashv a$, $d = 1$ must be the only possibility.

If $p \Dashv a$, then $p \Dashv p$ and $p \Dashv a$ for $p > 1$ (since any prime is > 1), so $\gcd(p, a) = p > 1$, which leads to a contradiction. So $p \nmid a$ must be true. □

32. If p, q are primes and $p \Dashv q$, then $p = q$. (prime can't divide other primes)

Proof. Since q is prime, if $k \Dashv q$, then $k = 1$ or $k = q$.

Since p is a prime (so $p \neq 1$) and $p \Dashv q$, $p = q$ must be true. □

33. Iff p is a prime, then $p \Dashv ab$ implies $p \Dashv a$ or $p \Dashv b$.

(Euclid's lemma)

Proof. ([25] p.15) ($\Rightarrow$) Assume that p is a prime and $p \Dashv ab$. If $p \Dashv a$ then we are done, so suppose that $p \nmid a$. By the property of prime, p and a are coprime. Also, we have $p \Dashv ab$. So by property of divisibility inheritance, we have $p \Dashv b$.

($\Leftarrow$) We need to show that if p is not a prime, then there always exists a, b such that $p \Dashv ab$ but $p \nmid a$ and $p \nmid b$.

If $p > 1$ is not a prime, then it must be composite, i.e., $p = ab$ for some $a, b > 1$. Thus $p \Dashv ab$ since $p \Dashv p$. Also, $p > a$ and $p > b$, so $p \nmid a$ and $p \nmid b$ (by property 6.5). □

34. If p is a prime and $p \Dashv a_1 a_2 \cdots a_n$, then $p \Dashv a_i$ for some $i \in \{1, 2, \ldots, n\}$.

(generalized Euclid's lemma)

Proof. ([25] p.15) We use induction on n. For the $n = 1$ base case the result is clear.

For the inductive step, assume the inductive hypothesis: that the lemma holds for $n = k$. We must show that it holds for $n = k + 1$.

For the LHS of $n = k{+}1$ case, assume that p is prime and $p \Dashv a_1 a_2 \cdots a_k a_{k+1}$. (Then we must show that the RHS of $n = k + 1$ case is true using the assumption that the lemma is true for for $n = k$.)

Write $a_1 a_2 \cdots a_k$ as a, and a_{k+1} as b. Then $p \Dashv a$ or $p \Dashv b$ by Euclid's lemma. If $p \Dashv a = a_1 \cdots a_k$ then by the induction hypothesis, $p \Dashv a_i$ for some $i \in \{1, \ldots, k\}$. If $p \Dashv b$ then $p \Dashv a_{k+1}$. So we can say that $p \Dashv a_i$ for some $i \in \{1, 2, \ldots, k + 1\}$. This verifies the lemma for $n = k + 1$. Hence by mathematical induction, it holds for all $n \leq 1$. □

35. If $n > 1$, then there exist a unique multi-set [11] of primes $\{p_1, \ldots, p_s\}$ such that $n = p_1 p_2 \cdots p_s$ and $p_1 \leq p_2 \leq \cdots \leq p_s$.

(Fundamental theorem of arithmetic)

Proof. ([25] p.16) First we prove the existence of said primes. We will use (strong) induction on n. The base step is $n = 2$: in this case, since 2 is prime we can take $s = 1$ and $p_1 = 2$.

For the inductive step, assume the hypothesis that the lemma holds for $2 \leq n \leq k$; we will show that it holds for $n = k + 1$. If $k + 1$ is prime then $s = 1$ and $p_1 = k + 1$ (then we are done). If $k + 1$ is composite then write $k + 1 = ab$ where $1 < a < k + 1$ and $1 < b < k + 1$. By the induction hypothesis there are primes $p_1, \ldots, p_u$ and $q_1, \ldots, q_v$ such that $a = p_1 \cdots p_u$ and $b = q_1 \cdots q_v$. This gives that $k + 1$ is a product of primes $k + 1 = ab = p_1 p_2 \cdots p_u q_1 q_2 \cdots q_v$, where $s = u + v$. Reorder the primes into ascending order, if necessary. The base step and the inductive step together give us that the statement is true for all $n > 1$. (Now forget the variables p, q)

Now we prove the uniqueness of said primes. We want to show that if $n = p_1 p_2 \cdots p_s$ for $s \geq 1$ with $p_1 \leq p_2 \leq \cdots \leq p_s$ (where the p_i s are primes), and also
$n = q_1 q_2 \cdots q_t$ for $t \geq 1$ with $q_1 \leq q_2 \leq \cdots \leq q_t$ (where the q_i s are primes), then $t = s$, and $p_i = q_i$ for all i between 1 and s.

[11] A multi-set allows duplicate elements, and the multi-set $\{a, b\} \neq \{a, a, b\}$.

The proof is by induction on s. In the $s = 1$ base case, $n = p_1$ is prime and we have $p_1 = q_1 q_2 \cdots q_t$. Now, t must be 1 or else this is a factorization of the prime p_1, and therefore $p_1 = q_1$.

Now assume the inductive hypothesis that the result holds for all s with $1 \leq s \leq k$. We must show that the result then holds for $s = k+1$. Assume that $n = p_1 p_2 \cdots p_{k+1}$ where $p_1 \leq p_2 \leq \cdots \leq p_{k+1}$, and also $n = q_1 q_2 \cdots q_t$ for $t \geq 1$ where $q_1 \leq q_2 \leq \cdots \leq q_t$. Clearly $p_{k+1} \Dashv n$, so $p_{k+1} \Dashv q_1 \cdots q_t$. Generalized Euclid's Lemma then gives that p_{k+1} divides some q_i . Since prime can't divide other primes, it must be that $p_{k+1} = q_i$. Hence $p_{k+1} = q_i \leq q_t$.

A similar argument shows that $q_t = p_j \leq p_{k+1}$. In detail, we have $q_t \Dashv n$, so $q_t \Dashv p_1 \cdots p_{k+1}$. Generalized Euclid's Lemma then gives that q_t divides some p_j. Since prime can't divide other primes, we have $q_t = p_j$. Hence $q_t = p_j \leq p_{k+1}$.

Therefore $p_{k+1} = q_t$.

To finish, cancel $p_{k+1} = q_t$ from the two sides of this equation.

$$p_1 p_2 \cdots p_k p_{k+1} = q_1 q_2 \cdots q_{t-1} q_t$$

Now the induction hypothesis applies: $k = t - 1$ and $p_i = q_i$ for $i = 1, \ldots, t-1$. (The induction hypothesis applies because there is only a shift of labelling for q_i. The original t in the hypothesis has become $t - 1$ in here.)

So the lemma holds also in the $s = k+1$ case, and so by mathematical induction it holds for all $s \geq 1$.

□

Note: The fundamental theorem of arithmetic basically says that every integer larger than 1 can be expressed as a unique prime factorization. An alternative formulation of the theorem is:

If $n > 1$, then $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ where $p_i \neq p_j$ if $i \neq j$.

We have basically collected the duplicate prime factors and make it into an exponent.

36. Let p and q be primes and $1 < a < pq$. If $a \Dashv pq$, then $a = p$ or $a = q$ (reverse Euclid's lemma)

Proof. $\Rightarrow$ Assume that $a \Dashv pq$. If $a \Dashv p$, then $a = 1$ or $a = p$ by the definition of a prime, but since $a > 1$ by the initial assumption, we have $a = p$.

If $a \nmid p$, then $a \neq 1$ or $a \neq p$. There are two cases: $1 < a < p$ or $p < a < pq$.

If $1 < a < p$, then $p \nmid a$ since a number's divisor can't be larger than itself. So a and p are coprime by the property of prime. Since $a \Dashv pq$ by the initial assumption, we have $a \Dashv q$ by the property of divisibility inheritance. Since q is prime and $a \neq 1$, we must have $a = q$.

If $p < a < pq$, then suppose that $p \Dashv a$. We have $a = kp$ and $pq = ma = m(kp) \;\Rightarrow\; q = mk$. Since q is prime, $k = 1$ or $k = q$. If $k = 1$, then $a = p$, which contradicts $p < a$. And if $k = q$, we have $a = pq$, which contradicts the initial constraint $a < pq$. The assumption $p \Dashv a$ leads to a contradiction either way, so $p \nmid a$ must be true. Similar to the argument above, we arrive at the conclusion that $a = q$.

Note: If $p = q$, it is not possible that $a \nmid p$, since if it is supposed that $a \nmid p$, then we will arrive at the conclusion that $1 < a < p$ or $p < a < pq$, but also $a = p$, which is a contradiction. Thus, if $p = q$, then $a \Dashv p$, which gives $a = p = q$. □

37. Let $P = \{p_1, p_2, \ldots, p_n\}$ be a multi-set of n primes and $a > 1$. Iff $a \Dashv p_1 p_2 \cdots p_n$, then $a = p_{s_1} p_{s_2} \cdots p_{s_t}$ for some t, where $1 \leq t \leq n$ and $\{p_{s_1}, p_{s_2}, \ldots, p_{s_t}\} \in \dbinom{P}{t}$.

(property of prime factors)

Note: The notation $\dbinom{P}{t}$ is defined as $\{A : |A| = t, A \subseteq P\}$ and in this context, means the multi-set of all k-element multi-subsets of P.

The 'then' statement basically says that a must be one of the primes or a product of some of the primes. The whole statement in plain words is "If a divides a number, then a is a factor of the prime factorization of that number" , and this is a generalization of the 'reverse Euclid's lemma'.

Proof. ($\Rightarrow$) If $a \Dashv p_1 p_2 \cdots p_n$, then $p_1 p_2 \cdots p_n = ka$ for some k. Suppose that $a > 1$ and $k > 1$. Let $a_1 a_2 \cdots a_t$ be the prime factorization of a and $m_1 m_2 \cdots m_r$ be the prime factorization of k , where $t, r \geq 1$. We have

$$p_1 p_2 \cdots p_n = ka = (a_1 a_2 \cdots a_t)(m_1 m_2 \cdots m_r)$$

By the funadmental theorem of arithmetic, there is only one unique prime factorization of $p_1 p_2 \cdots p_n$ (which is itself), so any prime factorization of the same number must be $p_1 p_2 \cdots p_n$ in some order. Note that $1 \leq t \leq n-1$ and $t + r = n$.

Thus, $a_i \in \{p_1, p_2, \ldots, p_n\}$ for all $i \in \{1, 2, \ldots, t\}$. So we have $a = a_1 a_2 \cdots a_t = p_{s_1} p_{s_2} \cdots p_{s_t}$ where $p_{s_i} = a_i$ (relabelling) and $\{p_{s_1}, p_{s_2}, \ldots, p_{s_t}\} \in \binom{\{p_1, p_2, \ldots, p_n\}}{t}$.

If $k = 1$ and $a = p_1 p_2 \cdots p_n$ instead, then the prime factorization of a is exactly $p_1 p_2 \cdots p_n$, so $a = p_{s_1} p_{s_2} \cdots p_{s_n}$ where $\{p_{s_1}, p_{s_2}, \ldots, p_{s_n}\} = \{p_1, p_2, \ldots, p_n\}$, thus a is just an arrangement of the prime factors.

($\Leftarrow$) If $a = p_{s_1} p_{s_2} \cdots p_{s_t}$ for some t, where $1 \leq t \leq n$ and $\{p_{s_1}, p_{s_2}, \ldots, p_{s_t}\} \in \binom{P}{t}$, then $p_1 p_2 \ldots p_n$ can be expressed in the form $p_{s_1}, p_{s_2}, \ldots, p_{s_t} k$ where k is the product of the remaining prime factors not appearing in a. So $a \Dashv p_1 p_2 \ldots p_n$.

□

38. Let p be a prime. Iff $d \Dashv p^k$, then $d = p^t$ where $0 \leq t \leq k$.
(property of prime power)

Proof. ($\Rightarrow$) The prime factorization of p^k is $\underbrace{p \ldots p}_{\text{k times}}$. Let P be the multi-set $\{\underbrace{p, p, \ldots, p}_{\text{k times}}\}$.

If $d \Dashv p^k$, then by property of prime factors, the prime factorization of d must be $1 \times \underbrace{p \ldots p}_{\text{t times}}$, where $0 \leq t \leq k$, which is p^t . If $t = 0$, then $d = p^0 = 1$ and we have $1 \Dashv p^k$, which is still true.

($\Leftarrow$) If $0 \leq t \leq k$, then since $p^k = p^t p^{k-t}$, we have $p^t \Dashv p^k$. □

39. If $\gcd(a, b) = 1$, then

$$\gcd(a, y) = 1 \text{ and } \gcd(b, x) = 1 \iff \gcd(ax + by, ab) = 1$$

(property of coprime linear combination)

Proof. [26] Assume that $\gcd(a, b) = 1$. We prove the contrapositive of each direction in the equivalence statement.

($\Rightarrow$) Suppose thus that there is a prime p such that $p \Dashv \gcd(ax + by, ab)$. Then

$\Rightarrow\ p \Dashv ab$ (GCD universal property)

$\Rightarrow\ p \Dashv a$ or $p \Dashv b$ (Euclid's lemma)

Without loss of generality, assume $p \Dashv a$.

Since $p \Dashv ax+by$ (GCD universal property) and $p \Dashv ax$, we have $p \Dashv by$ (property of divisible sum) .

Since $p \Dashv a$ and $\gcd(a, b) = 1$, $p \nmid b$. (Otherwise, $\gcd(a, b) \geq p > 1$)

Since $p \nmid b$ and p is prime, p and b must be coprime by the property of prime. Since $p \Dashv by$, we have $p \Dashv y$ by the property of divisibility inheritance. Thus $p \Dashv \gcd(a, y) \ \Rightarrow\ \gcd(a, y) > 1$.

Similarly, if $p \Dashv b$ instead, then $p \Dashv ax \ \Rightarrow\ p \Dashv x \ \Rightarrow\ \gcd(a, x) > 1$.

We have thus proven, under the hypothesis that $(a, b) = 1$; that

$$\gcd(ax + by, ab) > 1 \quad \Longrightarrow \quad \gcd(a, y) > 1 \text{ or } \gcd(b, x) > 1$$

($\Leftarrow$) Now suppose $\gcd(x, b) > 1$. We have $\gcd(x, b) \Dashv x$ and $\gcd(x, b) \Dashv b$, so $\gcd(x, b) \Dashv ax + by$ (property of linear combination)

Since $\gcd(x, b) \Dashv b$, we also have $\gcd(x, b) \Dashv ab$ (divisor divides number's multiple).

$\Rightarrow\ \gcd(ax + by, ab) \geq \gcd(x, b) > 1$. Analogously, $\gcd(a, y) > 1$ implies $\gcd(ax + by, ab) > 1$. □

40. If $b \Dashv a_i$ for all $i \in \{1, \ldots, n\}$, then $b \Dashv a_1x_1 + a_2x_2 + \ldots + a_nx_n$ ($\forall$ variables in $\mathbb{Z}$)

(generalized property of linear combinatioon)

Proof. Let $a_i = k_i b$. Then

$$\begin{aligned} a_1x_1 + a_2x_2 + \ldots + a_nx_n &= (k_1b)x_1 + (k_2b)x_2 + \ldots + (k_nb)x_n \\ &= b(k_1x_1 + k_2x_2 + \ldots + k_nx_n) \end{aligned}$$

$\Rightarrow\ b \Dashv a_1x_1 + a_2x_2 + \ldots + a_nx_n$ □

41. Let $a_1, a_2, \ldots a_n$ be non-zero integers. Then there exists $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ such that $a_1x_1 + a_2x_2 + \ldots + a_nx_n = \gcd(a_1, \ldots, a_n)$.
(generalized Bézout's identity)

Proof. [27] Given any non-zero integers $a_1, a_2, \ldots a_n$, let $S = \{a_1x_1 + a_2x_2 + \ldots + a_nx_n\ :\ x_1, \ldots, x_n \in \mathbb{Z}\ ,\ a_1x_1 + a_2x_2 + \ldots + a_nx_n > 0\}$ be the set of all positive linear combinations of $a_1, a_2, \ldots, a_n$. The set S is non-empty since we can set $x_1 = a_1$ and $x_i = 0$ for $i \neq 1$. So there exists an element $a_1^2 > 0$.

Since S is non-empty and has a lower bound of 0, it has a minimum element $d = a_1s_1 + a_2s_2 + \ldots + a_ns_n$ for some $s_1, \ldots, s_n \in \mathbb{Z}$.

First we prove that S is closed under subtraction, that is, for all $x, y \in S$, $x > y\ \Rightarrow\ x - y \in S$.

Suppose $x = a_1w_1 + a_2w_2 + \ldots + a_nw_n$ and $y = a_1z_1 + a_2z_2 + \ldots + a_nz_n$ with $x > y > 0$. Then

$$x - y = a_1(w_1 - z_1) + a_2(w_2 - z_2) + \ldots + a_n(w_n - z_n) > 0$$

Since $x - y$ is a positive linear combination of $a_1, a_2, \ldots, a_n$, $x - y$ is an element of S.

Now we prove that the minimum element d divides all elements in S . Suppose there exists at least one element in S that is not a multiple of d . Let ℓ be the minimum non-multiple of d . Then since $\ell > d$, we have $\ell - d \in S$ (since S is closed under subtraction) . But since $d \nmid \ell$, we have $d \nmid \ell - d$ (property of indivisible steps). We have found a new non-multiple $\ell - d$ that is smaller than the supposedly minimum non-multiple ℓ , which is a contradiction. So it must be that d divides all elements in S .

For all $i \in \{1, \ldots, n\}$, we have $a_i \in S$, seen by setting $x_i = 1$ and all $x_j = 0$ for $j \neq i$. Thus $d \Dashv a_i$ for all $i \in \{1, \ldots, n\}$.

If there is a common divisor c for which $c \Dashv a_i$ for all $i \in \{1, \ldots, n\}$, then $c \Dashv d = a_1s_1 + a_2s_2 + \ldots + a_ns_n$ (property of linear combination)

$\Rightarrow\ c \leq d$, making d necessarily the greatest common divisor of the a_i s.

□

42. Iff $c \Dashv a_i$ for all $i \in \{1, \ldots, n\}$, then $c \Dashv \gcd(a_1, a_2, \ldots, a_n)$ (generalized GCD universal property)

Proof. $(\Rightarrow)$ By generalized Bézout's identity, there exists $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ such that $a_1x_1 + a_2x_2 + \ldots + a_nx_n = \gcd(a_1, \ldots, a_n)$.

If $c \Dashv a_i$ for all $i \in \{1, \ldots, n\}$, then $c \Dashv a_1x_1 + a_2x_2 + \ldots + a_nx_n$ by generalized property of linear combination. $\Rightarrow\ c \Dashv \gcd(a_1, \ldots, a_n)$

$(\Leftarrow)$ Now we proof the converse. By definition, $\gcd(a_1, \ldots, a_n) \Dashv a_i$ for all $i \in \{1, \ldots, n\}$.

If $c \Dashv \gcd(a_1, \ldots, a_n)$, then $c \Dashv a_i$ for all $i \in \{1, \ldots, n\}$ by transitive property of divisibility.

□

43. $\gcd(a, b, c) = \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, c), b)$ (GCD associative property)

Proof. [28] ($d \Dashv a, b, c$ means $d \Dashv a$ and $d \Dashv b$ and $d \Dashv c$)

By the (generalized) GCD universal property we have: (for an arbitrary d)

$$d \Dashv \gcd(a, b, c) \Leftrightarrow d \Dashv a, b, c \Leftrightarrow d \Dashv \gcd(a, b), c \Leftrightarrow d \Dashv \gcd(\gcd(a, b), c)$$

Letting $d = \gcd(a, b, c)$, we have $\gcd(a, b, c) \Dashv \gcd(\gcd(a, b), c)$.

Letting $d = \gcd(\gcd(a, b), c)$, we have $\gcd(\gcd(a, b), c) \Dashv \gcd(a, b, c)$.

So we obtain $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$ (symmetry implies equality)

We can get the other equations by rearranging a, b, c.

$$d \Dashv \gcd(b, c, a) \Leftrightarrow d \Dashv b, c, a \Leftrightarrow d \Dashv \gcd(b, c), a \Leftrightarrow d \Dashv \gcd(\gcd(b, c), a)$$

$$d \Dashv \gcd(a, c, b) \Leftrightarrow d \Dashv a, c, b \Leftrightarrow d \Dashv \gcd(a, c), b \Leftrightarrow d \Dashv \gcd(\gcd(a, c), b)$$

□

44. Iff $\gcd(c, a_i) = 1$ for all $i \in \{1, \ldots, n\}$, then $\gcd(c,\ a_1a_2 \cdots a_n) = 1$

(generalized property of coprime sharing)

Proof. ($\Rightarrow$) We will prove by induction. For the $n = 2$ base case, we have $\gcd(c, a_1) = 1$ and $\gcd(c, a_2) = 1 \ \Rightarrow\ \gcd(c, a_1a_2) = 1$, which is the regular property of coprime sharing we proved earlier.

Assume that if $\gcd(c, a_i) = 1$ for all $i \in \{1, \ldots, k\}$, then $\gcd(c,\ a_1a_2 \cdots a_k) = 1$. Write $a_1a_2 \cdots a_k = b$.

For $n = k + 1$ case, if $\gcd(c, a_i) = 1$ for all $i \in \{1, \ldots, k + 1\}$, then by induction hypothesis, we have $\gcd(c,\ a_1a_2 \cdots a_k) = \gcd(c, b) = 1$

Since $\gcd(c, a_{k+1}) = 1$ and $\gcd(c, b) = 1$, by the regular property of coprime sharing, we have $\gcd(c, ba_{k+1}) = 1$. Thus $\gcd(c,\ a_1a_2 \cdots a_{k+1}) = 1$.

By mathematical induction, the implication is true for all integer $n > 1$.

($\Leftarrow$) We will prove by induction. For the $n = 2$ base case, we have $\gcd(c, a_1a_2) = 1 \ \Rightarrow\ \gcd(c, a_1) = 1$ and $\gcd(c, a_2) = 1$, which is the regular property of coprime sharing we proved earlier.

Assume that if $\gcd(c,\ a_1a_2 \cdots a_k) = 1$, then $\gcd(c, a_i) = 1$ for all $i \in \{1, \ldots, k\}$. Write $a_1a_2 \cdots a_k = b$.

For $n = k + 1$ case, if $\gcd(c,\ a_1a_2 \cdots a_{k+1}) = 1$, which means $\gcd(c,\ ba_{k+1}) = 1$, then $\gcd(c, b) = 1$ and $\gcd(c, a_{k+1})$ by the regular property of coprime sharing. By induction hypothesis, we have $\gcd(c, a_i) = 1$ for all $i \in \{1, \ldots, k\}$. Thus $\gcd(c, a_i) = 1$ for all $i \in \{1, \ldots, k + 1\}$

By mathematical induction, the implication is true for all integer $n > 1$. □

45. If $\gcd(a_i, a_j) = 1$ for all $i, j \in \{1, 2, \ldots, n\}$ where $i \neq j$, then $\gcd(a_i, \dfrac{a_1a_2 \cdots a_n}{a_i}) = 1$ for all i .

(property of pairwise coprime product)

Proof. Fix a particular i. If $\gcd(a_i, a_j) = 1$ for all $j \in \{1, 2, \ldots, n\}\backslash\{i\}$, then $\gcd(a_1,\ a_1a_2 \cdots a_{i-1}a_{i+1} \cdots a_n) = 1$ by the generalized property of coprime sharing.

Since $a_1a_2\cdots a_{i-i}a_{i+1}\cdots a_n = \dfrac{a_1a_2\cdots a_n}{a_i}$, we have $\gcd(a_i, \dfrac{a_1a_2\cdots a_n}{a_i}) = 1$. □

46. If $\gcd(a_i, a_j) = 1$ for all $i, j \in \{1, 2, \ldots, n\}$ where $i \neq j$, and $a_i \Dashv c$ for all $i \in \{1, 2, \ldots, n\}$, then $a_1a_2\cdots a_n \Dashv c$

(generalized property of divisor product)

Proof. We will prove by induction. For the base case $n = 2$, we have $\gcd(a_1, a_2) = 1$ and $a_1 \Dashv c$ and $a_2 \Dashv c \;\Rightarrow\; a_1a_2 \Dashv c$, which is the regular property of divisor product that we proved earlier.

Assume that if $\gcd(a_i, a_j) = 1$ for all $i, j \in \{1, 2, \ldots, k\}$ where $i \neq j$, and $a_i \Dashv c$ for all $i \in \{1, 2, \ldots, k\}$, then $a_1a_2\cdots a_k \Dashv c$. Write $a_1a_2\cdots a_k = b$.

For the $n = k + 1$ case, if $\gcd(a_i, a_j) = 1$ for all $i, j \in \{1, 2, \ldots, k + 1\}$ where $i \neq j$, and $a_i \Dashv c$ for all $i \in \{1, 2, \ldots, k + 1\}$, then by induction hypothesis, we have $a_1a_2\cdots a_k \Dashv c$ which means $b \Dashv c$.

Since $\gcd(a_{k+1}, a_i) = 1$ for all $i \in \{1, \ldots, k\}$, by generalized property of coprime sharing, we have $\gcd(a_{k+1},\; a_1a_2\cdots a_k) = 1$, which means $\gcd(a_{k+1}, b) = 1$. Since $\gcd(a_{k+1}, b) = 1$ and $a_{k+1} \Dashv c$ and $b \Dashv c$, by regular property of divisor product, we have $a_{k+1}b \Dashv c$. Thus $a_1a_2\cdots a_{k+1} \Dashv c$.

By mathematically induction, the implication is true for all $n > 1$. □

2.9.2 Properties of modulo

Now let's talk about the properties of the modulo operation, denoted $\%$, and the properties of **modular arithmetic**. Let me introduce some notations.

Notations (the bullet points are still not a part of notation)

- $\mathbb{Z}_n$ means the set "$\{0, 1, 2, \ldots, n - 1\}$"
- $a \% b$ means the operation "a mod b" / "the remainder of $a \div b$"

  (' $\%$ ' is an unconventional notation that I adopt (even though it's ugly) because it is one character only, unlike the conventional notation 'mod', which is 3 characters. This adoptation can shorten expressions slightly.)

(Mathematically, $a \% b$ is the remainder r when expressing a in the form (division algorithm) $a = bq + r$ where $q \in \mathbb{Z}$ and $r \in \mathbb{Z}_n$.)

(Note: n is called the **modulus** of the congruence.)

- $a \equiv b \pmod{n}$ means the statement "a and b are congruent modulo n"

  (Mathematically, $a \equiv b \pmod{n}$ if and only if $a \% n = b \% n$.)

- $a \not\equiv b \pmod{n}$ means the statement "a is not congruent to b modulo n"

  (Mathematically, $a \not\equiv b \pmod{n}$ if and only if $a \% n \neq b \% n$.)

- $\mathbb{Z}[x]$ means the set of all polynomials $f(x)$ with integer coefficients

  (Mathematically, $\mathbb{Z}[x] = \{c_0 + c_1x + c_2x^2 + \ldots + c_nx^n : c_n \in \mathbb{Z}, n \in \mathbb{N}\}$

Properties of modulo and congruences

(The variables mentioned are assumed to be integers unless stated otherwise.)

Here are some basic properties of the 'modulo' operation and congruences.

1. Iff $b \Dashv a$, then $a \% b = 0$ (a divisor leaves no remainder)

Proof. $b \Dashv a \;\Leftrightarrow\; a = kb \;\Leftrightarrow\; a = kb + 0 \;\Leftrightarrow\; a \% b = 0$ □

2. $(ka) \% a = 0$ (a number divides its multiple [alternate form])

Proof. $a \Dashv ka$ (a number divides its multiple) $\Leftrightarrow$ $(ka) \% a = 0$ (a divisor leaves no remainder) □

3. $a \% n = a \% (-n) = (-a) \% n = (-a) \% (-n)$ (negation property [of modulo])

Proof. If $a = qn + r$ for $q \in \mathbb{Z}$ and $r \in \mathbb{Z}_n$, then:

$a = (-q)(-n) + r$

$(-a) = (-q)n + r$

$(-a) = q(-n) + r$

$\Rightarrow\; a \% n = a \% (-n) = (-a) \% n = (-a) \% (-n) = r$ □

4. $(a \% n) \% n = a \% n$ (simplification of modulo)

Proof. Let $r = a \% n$. We have $0 \leq r < n$. So $r = 0n + r$ and thus $r \% n = r$. Thus $a \% n \% n = a \% n$ (We can omit the bracket.) □

5. $a \equiv a \% n \pmod{n}$ (remainder congruence)

Proof. $a \% n = (a \% n) \% n$ (simplification of modulo)
$\Rightarrow\ a \equiv a \% n \pmod{n}$ □

6. $a \equiv a \pmod{n}$ (reflexive property)

Proof. $a \% n = a \% n$ □

7. Iff $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$ (symmetric property)

Proof. $a \equiv b \pmod{n} \ \Leftrightarrow\ a \% n = b \% n \Leftrightarrow\ b \% n = a \% n$
$\Rightarrow\ b \equiv a \pmod{n}$ □

8. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
(transitive property)

Proof. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$
$\Rightarrow\ a \% n = b \% n$ and $b \% n = c \% n$
$\Rightarrow\ a \% n = c \% n \ \Rightarrow\ a \equiv c \pmod{n}$ □

8.5. If $a \equiv c \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv b \pmod{n}$.
(another transitive property)

Proof. If $a \equiv c \pmod{n}$ and $b \equiv c \pmod{n}$, then
$\Rightarrow\ a \equiv c \pmod{n}$ and $c \equiv b \pmod{n}$ (reflexive property)
$\Rightarrow\ a \equiv b \pmod{n}$ (transitive property) □

Note: Now we just call this the transitive property.

9. $a \equiv b \pmod{n} \ \Leftrightarrow\ a \equiv -b \pmod{n} \ \Leftrightarrow\ -a \equiv b \pmod{n}$
$\Leftrightarrow\ -a \equiv -b \pmod{n}$ (negation property [of congruence])

Proof. By the negation property of modulo,

$a \% n = b \% n \;\Leftrightarrow\; a \% n = (-b) \% n \;\Leftrightarrow\; (-a) \% n = b \% n$
$\Leftrightarrow\; (-a) \% n = (-b) \% n$ □

10. If $r = a \% n$, then $ak \equiv rk \pmod{n}$ (remainder property)

Proof. $r = a \% n \;\Rightarrow\; a = qn + r$ for $q \in \mathbb{Z}$ and $r \in \mathbb{Z}_n$.

$\Rightarrow\; ak = (qn + r)k = (kq)n + rk$, and by the division algorithm,

$$rk = q_2 n + r_2 \qquad \ldots(*)$$

for some $q_2 \in \mathbb{Z}$ and $r_2 \in \mathbb{Z}_n$.

Thus,

$$\begin{aligned} ak &= (kq)n + rk \\ &= (kq)n + q_2 n + r_2 \\ ak &= (kq + q_2)n + r_2 \qquad \ldots(**) \end{aligned}$$

By (*) and (**), $ak \% n = rk \% n = r_2 \;\Rightarrow\; ak \equiv rk \pmod{n}$. □

11. Iff $a \equiv b \pmod{n}$, then $n \Dashv (a - b)$ and $n \Dashv (b - a)$.
(difference property)

Proof. ([25] p.31) Write $a = nq_a + r_a$ and $b = nq_b + r_b$ for some q_a, q_b, r_a, and r_b, with $0 \leq r_a, r_b < n$. Subtracting gives

$$a - b = n(q_a - q_b) + (r_a - r_b) \qquad \ldots(*)$$

. Observe that the restrictions on the remainders imply that $-n < r_a - r_b < n$, and so $r_a - r_b$ is not a multiple of n unless $r_a - r_b = 0$.

($\Rightarrow$) If a and b are congruent modulo n , then $r_a = r_b$, which implies that $a - b = n(q_a - q_b)$, which in turn gives that n divides $a - b$.

Then $n \Dashv (a - b) \;\Leftrightarrow\; n \Dashv -(b - a) \;\Leftrightarrow\; n \Dashv (b - a)$.

($\Leftarrow$) The implications in the prior paragraph reverse: if n divides $a - b$, then $a - b = nk$ for some $k \in \mathbb{Z}$. Combining this with equation (*) gives

$$nk = n(q_a - q_b) + (r_a - r_b)$$

$$r_a - r_b = n(k - (q_a - q_b))$$

Since $r_a - r_b$ is a multiple of n, we must have that $r_a - r_b = 0$ by the observation in the first paragraph, and therefore $r_a = r_b$.

□

12. If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{n}$ (scaling property of congruence)

Proof. $a \equiv b \pmod{n} \;\Rightarrow\; n \Dashv a - b$ (difference property)

$\Rightarrow\; n \Dashv k(a-b)$ (divisor divides a number's multiple)

$\Rightarrow\; n \Dashv ka - kb$

$\Rightarrow\; ka \equiv kb \pmod{n}$ (differnece property)

□

13. If $a \equiv b \pmod{n}$, then $a+kn \equiv b \pmod{n}$ (property of modulus steps)

Proof. $\Rightarrow\; n \Dashv a-b \Rightarrow\; n \Dashv a-b+kn$ (property of linear combination)

$\Rightarrow\; n \Dashv (a+kn)-b \Rightarrow\; a+kn \equiv b \pmod{n}$ □

14. If $as \equiv b \pmod{n}$ and $s \equiv t \pmod{n}$, then $at \equiv b \pmod{n}$

(substitution property)

Proof. $\Rightarrow\; n \Dashv as - b$ and $n \Dashv s - t$ (difference property)

$\Rightarrow\; n \Dashv (as-b) - a(s-t)$ (property of linear combination)

$\Rightarrow\; n \Dashv at - b$ (simplifying)

$\Rightarrow\; at \equiv b \pmod{n}$ (difference property) □

15. If $as \equiv b \pmod{n}$, then $a(s+kn) \equiv b \pmod{n}$

(reduction property)

Proof. $\Rightarrow\; n \Dashv as - b$ (difference property)

$\Rightarrow\; n \Dashv (as-b) + ak(n)$ (property of linear combination)

$\Rightarrow\; n \Dashv a(s+kn) - b$ (rearranging)

$\Rightarrow\; a(s+kn) \equiv b \pmod{n}$ (difference property) □

16. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a+c \equiv b+d \pmod{n}$ and $a-c \equiv b-d \pmod{n}$.

(additive property)

Proof. ([25] p.33) $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

$\Rightarrow\ n \Dashv a-b$ and $n \Dashv c-d$ (difference property)

$\Rightarrow\ n \Dashv (a-b)+(c-d)$ (property of linear combination)

$\Rightarrow\ n \Dashv (a+c)-(b+d)$ (rearranging)

$\Rightarrow\ a+c \equiv b+d \pmod{n}$ (difference property)

For the minus case, let $c' = -c$ and $d' = -d$. Then

$\Rightarrow\ a \equiv b \pmod{n}$ and $c' \equiv d' \pmod{n}$, so

$\Rightarrow\ a+c' \equiv b+d' \pmod{n}$

$\Rightarrow\ a-c \equiv b-d \pmod{n}$ □

17. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$

(multiplicative property)

Proof. ([25] p.33) $\Rightarrow\ n \Dashv a-b$ and $n \Dashv c-d$ (difference property)

$\Rightarrow\ n \Dashv c(a-b)+b(c-d)$ (property of linear combination)

Since $c(a-b)+b(c-d) = ac-bd$, we have $n \Dashv ac-bd$.

$\Rightarrow\ ac \equiv bd \pmod{n}$ (difference property) □

18. If $a \equiv b \pmod{n}$, then $a^m \equiv b^m \pmod{n}$ for all $m \in \mathbb{N}$

(power property)

Proof. ([25] p.33) We prove this by induction on m. If $m = 0$, then we have $1 \equiv 1 \pmod{n}$, which is obviously true. If $m = 1$, the result is true by the assumption that $a \equiv b \pmod{n}$. Assume that the result holds for $m = k$. Then we have $a^k \equiv b^k \pmod{n}$. This, together with $a \equiv b \pmod{n}$ using multiplicative property, gives that $aa^k \equiv bb^k \pmod{n}$. Hence $a^{k+1} \equiv b^{k+1} \pmod{n}$ and the result holds in the $n = k+1$ case. So the result holds for all $n \geq 0$, by induction. □

19. If $f(x) \in \mathbb{Z}[x]$ (i.e. $f(x)$ is a polynomial with integer coefficients) and $a \equiv b \pmod{n}$, then $f(a) \equiv f(b) \pmod{n}$

(polynomial property)

Proof. ([25] p.33) Let $f(x) = c_n x^n + \cdots + c_1 x + c_0$. We prove by induction on the degree of the polynomial n that if $a \equiv b \pmod{n}$ then $c_m a^m + \cdots + c_0 \equiv c_m b^m + \cdots + c_0 \pmod{n}$. For the degree $m = 0$ base case, by the reflexivity of congruence we have that $c_0 \equiv c_0 \pmod{n}$.

For the induction assume that the result holds for $n = k$. Then we have

$$c_k a^k + \cdots + c_1 a + c_0 \equiv c_k b^k + \cdots + c_1 b + c_0 \pmod{n}. \qquad (*)$$

By power property we have $a^{k+1} \equiv b^{k+1} \pmod{n}$. Since $c_{k+1} \equiv c_{k+1} \pmod{n}$, by multiplicative property we have

$$c_{k+1} a^{k+1} \equiv c_{k+1} b^{k+1} \pmod{n}. \qquad (**)$$

Now we can apply additive property to $(*)$ and $(**)$ to obtain

$$c_{k+1} a^{k+1} + c_k a^k + \cdots + c_0 \equiv c_{k+1} b^{k+1} + c_k b^k + \cdots + c_0 \pmod{n}.$$

So by induction the result holds for all $m \geq 0$. □

20. If $s = a_1 + a_2 + \ldots + a_m$ and $a_i \equiv r_i \pmod{n}$ for all $i \in \{1, \ldots, m\}$, then $s \equiv r_1 + r_2 + \ldots + r_m \pmod{n}$ (generalized additive property)

Proof. We will use proof by induction. For the base case $m = 1$, we have $s = a_1$ and $a_1 \equiv r_1 \pmod{n} \Rightarrow s \equiv r_1 \pmod{n}$, which can be seen by direct substitution.

Assume that if $s = a_1 + a_2 + \ldots + a_k$ and $a_i \equiv r_i \pmod{n}$ for all $i \in \{1, \ldots, k\}$, then $s \equiv r_1 + r_2 + \ldots + r_k \pmod{n}$.

For the $m = k+1$ case, if $s = a_1 + a_2 + \ldots + a_{k+1}$ and $a_i \equiv r_i \pmod{n}$ for all $i \in \{1, \ldots, k+1\}$, then $a_1 + a_2 + \ldots + a_k \equiv r_1 + r_2 + \ldots + r_k \pmod{n}$ by induction hypothesis.

Since $a_{k+1} \equiv r_{k+1} \pmod{n}$, we have

$$a_1 + a_2 + \ldots + a_k + a_{k+1} \equiv r_1 + r_2 + \ldots + r_k + r_{k+1} \pmod{n}$$

by regular additive property. So $s \equiv r_1 + r_2 + \ldots + r_k + r_{k+1} \pmod{n}$.

By mathematical induction, the implication is true for all positive integers m . □

21. Let $n \geq 2$. If a and n are coprime, then there exists a unique integer a^* such that $aa^* \equiv 1 \pmod{n}$ and $0 < a^* < n$.

(property of invertibles)

Note: a^* is called the inverse of a modulo n.

Proof. ([25] p.37) (Existence of inverse) Assume that $\gcd(a, n) = 1$. Bezout's identity applies to give $s, t \in \mathbb{Z}$ such that $as + nt = 1$. Hence $as - 1 = n(-t)$, that is, $n \Dashv as - 1$ and so $as \equiv 1 \pmod{n}$ by difference property.

Note that $n \nmid s$ because otherwise, $s = nk$ for some k and
$as + nt = a(nk) + nt = n(ak + t) \neq 1$ since $n > 1$.

Accordingly, let $a^* = s \mathbin{\%} n$ so that $0 < a^* < n$. Then $a^* \equiv s \pmod{n}$ (by remainder congruence) so $aa^* \equiv 1 \pmod{n}$ (by substitution property).

(Uniqueness of inverse) To show uniqueness, assume that $ac \equiv 1 \pmod{n}$ and $0 < c < n$. Then $ac \equiv aa^* \pmod{n}$ (by transitive property). So $cac \equiv caa^* \pmod{n}$. Use the fact that $ca \equiv 1 \pmod{n}$ and substitution property on both sides to obtain $c \equiv a^* \pmod{n}$. Because both c and a^* are in $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, it follows that $c = a^*$. □

22. Let c, n be coprimes. If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n}$

(property of cancellation)

Proof. ([25] p.38) If $\gcd(c, n) = 1$, then it has an inverse c^* modulo n, such that $c^*c \equiv 1 \pmod{n}$. Since $ca \equiv cb \pmod{n}$, $c^*ca \equiv c^*cb \pmod{n}$ by the scaling property of congruence. But $c^*c \equiv 1 \pmod{n}$ so $c^*ca \equiv a \pmod{n}$ and $c^*cb \equiv b \pmod{n}$. By reflexivity and transitivity,
$a = c^*cb \pmod{n}$ and $b = c^*cb \pmod{n}$, which yields $a \equiv b \pmod{n}$ by another transitive property. □

23. Suppose that $n_1, \ldots, n_k$ are pairwise coprime (that is, $\gcd(n_i, n_j) = 1$ whenever $i \neq j$). Then the system of congruences (with x as the unknown)

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a unique solution modulo $n_1 n_2 \ldots n_k$.

(Chinese remainder theorem)

Proof. ([25] p.52) Let $N = n_1 n_2 \cdots n_k$ and for $i \in \{1, \ldots, k\}$ let $N_i = N/n_i = n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_k$. Observe that $\gcd(N_i, n_i) = 1$ (by the property of pairwise coprime product) , so by the property of invertibles, there exists a unique x_i where $0 < x_i < n_i$ for each i such that $N_i x_i \equiv 1 \pmod{n_i}$.

Now consider the number

$$s_0 = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_k N_k x_k.$$

We claim that s_0 solves the system. For, consider the i-th congruence $x \equiv a_i \pmod{n_i}$. Because n_i divides N_j when $i \neq j$, we have $N_j \equiv 0 \pmod{n_i}$, thus $a_j N_j x_j \equiv 0 \pmod{n_i}$ when $i \neq j$ by scaling property. Thus, by generalized addition property, we have that

$$s_0 \equiv 0 + \ldots + 0 + a_i N_i x_i + 0 + \ldots + 0 \pmod{n_i}$$

$$s_0 \equiv a_i N_i x_i$$

Since x_i was chosen because of the property that $N_i x_i \equiv 1 \pmod{n_i}$, we have that $s_0 \equiv a_i \cdot 1 \equiv a_i \pmod{n_i}$ (by substitution property), as claimed.

To finish we must show that the solution is unique modulo N. Suppose that there are two solutions u and v to the system of congruences, so that for each $i \in \{1, \ldots, k\}$ we have that $u \equiv v \equiv a_i \pmod{n_i}$. Restated, for each i we have that $n_i \Dashv (u - v)$.

We can now show that $n_1 n_2 \ldots n_k \Dashv (u-v)$. We have that $\gcd(n_i, n_j) = 1$ for all $i, j \in \{1, \ldots, k\}$ where $i \neq j$, and $n_i \Dashv (u - v)$ for all $i \in \{1, \ldots, k\}$. By generalized property of divisor products, we conclude that $n_1 n_2 \cdots n_k \Dashv (u - v)$, which means

$$u \equiv v \pmod{n_1 n_2 \cdots n_k}$$

Thus, the solution is unique modulo $n_1 n_2 \cdots n_k$, which means $r = u \,\%\, n_1 n_2 \cdots n_k = v \,\%\, n_1 n_2 \cdots n_k$ is the unique solution where $0 \le r < n_1 n_2 \cdots n_k$. □

2.9.3 Probability problems in number theory

Let's try some problems of probability × number theorey.

Problem 64. In a box, there are 1000 cards labelled from 1 to 1000. If I randomly draw a card from the box, what is the probability that the number on it is divisible by 6 or divisible by 8 (or both)?

(Difficulty level: 4)

Solution 64. From 1 to 1000, the total number of integers divisible by 6 is $\lfloor \frac{1000}{6} \rfloor = 166$.

The total number of integers divisible by 8 is $\frac{1000}{8} = 125$. We have double counted the multiples of $\text{lcm}(6, 8) = 24$, so we subtract those: $\lfloor \frac{1000}{24} \rfloor = 41$. So

$$P(\text{divisible by 6 or 8}) = \frac{166 + 125 - 41}{1000} = \boxed{\frac{1}{4}}.$$

That was just an appetizer. Here's the real deal:

Problem 65. Two integers a and b are picked at random from 1 to 1 000 000 inclusive without replacement. What is the probability that $\dfrac{a}{b}$ is a reduced fraction?

(Difficulty level: 9) [29] (Project Euler Problem 72 Modified)

2.9.4 Euler's totient function

Discussion 65. There are a total of $C_2^{1\,000\,000}$ combinations of integers a, b. If $\dfrac{a}{b}$ is a reduced fraction, then a, b are coprime, so we need to find all combinations of a, b such that $\gcd(a, b) = 1$.

Let me introduce the **Euler's totient function** [30], which counts the positive integers up to a given integer n that are coprime to n, and it is denoted $\phi(n)$. In other words, it counts the number of integers k in the range $1 \leq k \leq n$ for which $\gcd(k, n) = 1$.

For example, for $n = 9$, there are six numbers 1, 2, 4, 5, 7 and 8 that are all coprime to 9, but the other three numbers in this range, 3, 6, and 9 are not, since gcd(9, 3) = gcd(9, 6) = 3 and gcd(9, 9) = 9. Therefore, $\phi(9) = 6$.

As another example, $\phi(1) = 1$ since for $n = 1$ the only integer in the range from 1 to n is 1 itself, and gcd(1, 1) = 1.

Note that when $n > 1$, $\phi(n)$ counts the number of combinations of two coprime integers, for which one of the number is n, and the other number is less than n. So the sum $\phi(2) + \phi(3) + \ldots + \phi(1\,000\,000)$ is the total number of combinations of two coprime integers ranging from 1 to 1 000 000. ($\phi(1)$ is excluded since it repeats two 1's.)

There are some properties of that ϕ function that we want to explore, such as the fact that it is a **multiplicative function** [12]

Preposition. If m, n are coprime, then $\phi(mn) = \phi(m) \cdot \phi(n)$

Proof. [31] Let m, n be coprimes. Consider the set $\mathbb{Z}_{mn} = \{0, 1, 2, \ldots, mn - 1\}$ and the sets $\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\}$ and $\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$. We want to show that $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$, that is, $\mathbb{Z}_{mn}$ has the same number of elements as $\mathbb{Z}_m \times \mathbb{Z}_n$ (even though it is obvious).

Define a function $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, i.e., f maps $\mathbb{Z}_{mn}$ to the set $\mathbb{Z}_m \times \mathbb{Z}_n$. For each a in $\mathbb{Z}_{mn} = \{0, 1, 2, \ldots, mn - 1\}$, define $f(a) = (c, d)$ where $c \in \mathbb{Z}_m$ with $c \equiv a \pmod{m}$ and $d \in \mathbb{Z}_n$ with $d \equiv a \pmod{n}$, and (c, d) is an ordered pair.

Note that c, d are necessarily unique for the same a (so the function is valid) because we have $0 \leq c < m$, so $c = c \,\%\, m = a \,\%\, m$, and similarly, $0 \leq d < n$, so $d = d \,\%\, n = a \,\%\, n$.

To show that f is a bijection, let $(c, d) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Consider the equations $x \equiv c \pmod{m}$ and $x \equiv d \pmod{n}$. By Chinese remainder theorem, these two equations have a solution a that is unique modulo mn , i.e. there is a unique solution a where $0 \leq a < mn$, which means there is exactly one $a \in \mathbb{Z}_{mn}$ such that $f(a) = (c, d)$ for every $(c, d) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Combined with the fact that each $a \in \mathbb{Z}_{mn}$ can only be mapped to exactly one $(c, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, we conclude that f is a bijection.

This means that $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$.

[12] In number theory, a multiplicative function $f(n)$ has the property that $f(1) = 1$ and $f(mn) = f(m)f(n)$ whenever m and n are coprime.

Now, let m, n still be coprimes. Let $\mathbb{Z}_{mn}^*$ be the set of all elements in $\mathbb{Z}_{mn}$ that is coprime to mn . Mathamatically, $\mathbb{Z}_{mn}^* = \{\gcd(a, mn) = 1 \, : \, a \in \mathbb{Z}_{mn}\}$. Let $\mathbb{Z}_m^*$ and $\mathbb{Z}_n^*$ be defined similarly. Note that $|\mathbb{Z}_m^*| = \phi(m)$, $|\mathbb{Z}_n^*| = \phi(n)$ and $|\mathbb{Z}_{mn}^*| = \phi(mn)$.

We want to show that $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \times |\mathbb{Z}_n^*|$, which means $\phi(mn) = \phi(m)\phi(n)$.

The same mapping f defined above is used. We show that when the domain of f is restricted to the set $\mathbb{Z}_{mn}^*$, it is a bijection from $\mathbb{Z}_{mn}^*$ onto the set $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$. First, we show that for any $a \in \mathbb{Z}_{mn}^*$, $f(a)$ is indeed in $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$. To see this, note that a and mn are coprime. So it must be that a and m are coprime too and that a and n are coprime (property of coprime sharing).

The function f is one-to-one (an injection) as shown above. The remaining piece is that for each $(c, d) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$, there is some $a \in \mathbb{Z}_{mn}^*$ such that $f(a) = (c, d)$. As in the proof of $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$ above, there is some $a \in \mathbb{Z}_{mn}$ such that $f(a) = (c, d)$ for every (c, d). Note that c, m are coprime and d, n are coprime. Since $c \equiv a \pmod{m}$, $a = c + km$ for some k , so $\gcd(c + km, m) = 1$ (property of coprime steps), which means that a and m are coprime. By similar reasoning, a and n are coprime. This means that a and mn are coprime (property of coprime sharing), which means $a \in \mathbb{Z}_{mn}^*$. Thus the function f is a one-to-one from $\mathbb{Z}_{mn}^*$ onto $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ (a bijection), so we have $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \times |\mathbb{Z}_n^*|$, and

$$\phi(mn) = \phi(m)\phi(n)$$

□

We can visualize this mapping by listing the elements in $\mathbb{Z}_{mn}$ in an $n \times m$ array. (Actually I haven't completed this yet, so we can visualize nothing from this.)

$$\begin{array}{ccccc}
0 & 1 & 2 & \ldots & m-1 \\
m & m+1 & m+2 & \ldots & 2m-1 \\
2m & 2m+1 & 2m+2 & \ldots & 3m-1 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(n-1)m & (n-1)m+1 & (n-1)m+2 & \ldots & mn-1
\end{array}$$

Preposition (Value of ϕ for a prime power)**.** If p is a prime and $k \geq 1$, then

$$\phi(p^k) = p^k - p^{k+1} = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$$

Proof. [32] Since p is a prime number, $d \Dashv p^k$ if and only if $d = p^t$ where $0 \leq t \leq k$ (property of prime power). So for an arbitrary m, the only possible values of $\gcd(p^k, m)$ are $1, p, p^2, \ldots, p^k$. By generalized property of coprime sharing, $\gcd(p^k, m) = 1$ if and only if $\gcd(p, m) = 1$. The contrapositive is that if $\gcd(p, m) > 1$, then $\gcd(p^k, m) > 1$. By the property of prime, the only way to have $\gcd(p, m) > 1$ and thus $\gcd(p^k, m) > 1$ is if m is a multiple of p, that is, $m \in \{p, 2p, 3p, \ldots, p^{k-1}p = p^k\}$, and there are p^{k-1} such multiples not greater than p^k. Therefore, the other $p^k - p^{k-1}$ numbers in $\{1, 2, \ldots, p^k\}$ are all relatively prime to p^k. □

Now how do we go from here? Recall the fundamental theorem of arithmetic, which states that $n > 1$ there is a unique expression $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$, where $p_1 < p_2 < \ldots < p_t$ are prime numbers and each $k_i \geq 1$. (The case $n = 1$ corresponds to the empty product.) Repeatedly using the multiplicative property gives: [32]

$$\begin{aligned}
\phi(n) &= \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_t^{k_t}) \\
&= p_1^{k_1-1}(p_1 - 1)\, p_2^{k_2-1}(p_2 - 1) \cdots p_t^{k_t-1}(p_t - 1) \\
&= p_1^{k_1}(1 - \frac{1}{p_1}) p_2^{k_2}(1 - \frac{1}{p_2}) \cdots p_t^{k_t}(1 - \frac{1}{p_t}) \\
&= p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_t}) \\
&= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_t}) \\
&= n \prod_{p \Dashv n} (1 - \frac{1}{p})
\end{aligned}$$

Thus, we see that $\phi(n)$ is n times the product of 1 minus the reciprocal of each distinct prime factors of n . Note that the big pi notation $\prod$ is the product version of the sigma notation $\sum$.

Theorem 2.15. If $\phi(n)$ is the number of positive integers not larger than n that are coprime to n , then

$$\phi(n) = n \prod_{p \Dashv n} (1 - \frac{1}{p})$$

where the product is over the distinct prime numbers that divide n .

To check that it indeed works, use the formula to find $\phi(12)$:

$$\phi(12) = 12(1 - \frac{1}{2})(1 - \frac{1}{3}) = 4$$

We can verify that there are only 4 coprime positive integers smaller than 12, which are 1, 5, 7, 11 .

Having obtained a nice formula that can speed up our calculation, now we can finally return to the problem.

Problem 66. (Restated) Two integers a and b are picked at random from 1 to 1 000 000 inclusive without replacement. What is the probability that $\frac{a}{b}$ is a reduced fraction?

(Difficulty level: 9) [29] (Project Euler Problem 72 Modified)

Solution 66. We want to find the number of combinations of two coprime integers in the range $\{1, 2, \ldots, 1\,000\,000\}$, which is given by the sum

$$\phi(2) + \phi(3) + \ldots + \phi(1\,000\,000)$$

where ϕ is Euler's totient function. Recall the formula

$$\phi(n) = n \prod_{p \Dashv n} (1 - \frac{1}{p}) = n \prod_{p \Dashv n} (\frac{p-1}{p})$$

For $k \in \mathbb{Z}^+$, note that every $2k$ (even number) has a prime factor 2, which means every $\phi(2k)$ has a factor $(1 - \frac{1}{2})$ in the product. Similarly, every $3k$ has a prime factor 3, which means every $\phi(3k)$ has a factor $(1 - \frac{1}{3})$. Generally, for a prime p , every pk has a prime factor p, which means every $\phi(pk)$ has a factor $(1 - \frac{1}{p})$. Moreoever, note that every $\phi(k)$ contains k in the product.

Thus, we can first make a list which contains k as the k th element in a computer. Then we can multiply every $2k$ th element in the list by $(1 - \frac{1}{2})$, and then every $3k$ th element in the list by $(1 - \frac{1}{3})$, and then every $5k$ th element in the list by $(1 - \frac{1}{5})$, and so on. Note that we don't need to multiply every $4k$ th element by something because 4 is not a prime. So for every prime p in $\{1, \ldots, 1\,000\,000\}$, we multiply every pk th element by $(1 - \frac{1}{p})$. This method is similar to the sieve of Eratosthenes. After all the multiplying, we will be left with a list that contains $\phi(k)$ in the k th element. Then we can simply sum the list from the 2th element to the 1 000 000 th element, which will give us the number of desired outcomes.

Moreoever, note that when we have a prime p as the p th element in the list, it will not be multiplied by any $(1 - \frac{1}{q})$ for any prior primes q where $2 \leq q < p$, because primes are pretty good at avoiding multiples of numbers. So the p th element will still contain the number p just before we need to multiply every pk th element by $(1 - \frac{1}{p})$. As for any composite number c, it must be some prime number's multiple and will get multiplied by a factor $(1 - \frac{1}{q})$ where $q < c$ at some point. Thus we can check whether the n th element is n before multiplying multiples of n. If yes, then prime, and go ahead, else not prime and skip that number. This can minimize the effort of checking for primes.

Using python code to implement this:

```
phi = list(range(1000001))
for k in range(2, 1000001):
    if phi[k] == k:
        for i in range(k, 1000001, k):
                phi[i] = phi[i] * (k - 1) // k
print(sum(phi[2:]))
```

And we get

```
    303963552391
```

The total number of outcomes is $C_2^{1000000} = 499999500000$. So

P(reduced fraction)= $\boxed{\frac{303\,963\,552\,391}{499\,999\,500\,000}}$

2.10 Generating functions

Sometimes, the number of ways to do something is pretty hard to count, and the regular counting methods do not help us much. There is an alternative way to count the number of ways, using **generating functions**. [33] (It is sort of like black magic.)

When we want to find the number of ways to do something involving n objects, such as the number of permutations of n objects, number of subsets of an n-element set, etc, we can form a sequence of numbers $a_0, a_1, a_2, \dots$, where a_n is the number of ways to do something involving n objects. A generating function essentially encodes the sequence in a polynomial:

$$A(x) = \sum_{n \geq 0} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$$

As we can see, the coefficient of the n th power of x is a_n , which is the number of ways to do stuff involving n objects. Here, the variable x does not stand for anything, and only serves as a placeholder for keeping track of the coefficients of x^n.

For example, the generation function associated with the number of subsets of an n-element set is $\sum_{n \geq 0} 2^n x^n = 1 + 2x + 4x^2 + 8x^3 + \dots$ If we want to find the number of subsets of an 6-element set, we look for the coefficient of x^6, which is 64 in this case.

What if we want to find the number of ways to obtain a sum of n when throwing a 6-sided dice and a 8-sided dice?

First, let's consider the generating function $A(x)$ of the 6-sided dice only. There is only one way to get each number, so

$$A(x) = x + x^2 + x^3 + x^4 + x^5 + x^6$$

Similarly, the generating function $B(x)$ of the 8-sided dice is:

$$B(x) = x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8$$

To find the generating function $C(x)$ associated with the number of sums of the two dice, we can make use of the property of exponents: $x^a \cdot x^b = x^{a+b}$. So we can just multiply $A(x)$ and $B(x)$ together to get $C(x)$.

$$C(x) = (x + x^2 + x^3 + x^4 + x^5 + x^6) \times (x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8)$$

This works because when we expand $A(x) \cdot B(x)$, we choose one term x^a from $A(x)$ and one term x^b from $B(x)$ and multiply them together, which is done by adding the exponents of the two terms. We get x^{a+b}, which represents 1 way to obtaining a sum of $a+b$. There are many other ways to obtain x^{a+b} when expanding $A(x) \cdot B(x)$, and when we group the like terms together, the coefficient represents the total number of ways to obtain a sum of $a+b$.

For instance, getting the sum 5 by getting 2 from the first dice and 3 from the second dice is accounted by the multiplication of the monomial x^2 from the first parenthesis with monomial x^3 from the second parenthesis , etc. Multiplying this out, we get

$$C(x) = x^2 + 2x^3 + 3x^4 + 4x^5 + 5x^6 + 6x^7 + 6x^8$$

$$+6x^9 + 5x^{10} + 4x^{11} + 3x^{12} + 2x^{13} + x^{14}$$

We are now ready for the challenging puzzle (inspired by 3Blue1Brown).

2.10.1 A puzzling puzzle

Problem 67. I am playing a game, in which I flip a fair coin 2000 times, and if I get a head in the i th coin flip, I will get $\$i$. If I get a tail instead, I get no money. I have gained a total of $\$X$ after playing the game. What is the probability that X is divisible by 5?

(Express the answer as a **reduced fraction**.)

(Difficulty level: 9) [34]

Solution 67a. There are 2^{2000} possible outcomes. Finding the number of desired outcomes (denoted by S) is equivalent to finding the number of subsets of
$E = \{1, \ldots, 2000\}$ that have a sum divisible by 5. The generating function associated with this is

$$A(x) = (1+x)(1+x^2)(1+x^3)\ldots(1+x^{2000})$$

When we expand this out, we get

$$A(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{2001000} x^{2001000}$$

where $2001000 = 1 + 2 + 3 + \ldots + 2000$. Let's denote this number by N.

Each coefficient a_n of x^n represents the number of subsets of E whose elements sum up to n . If, say, we want to look for the number of subsets whose elements sum up to 10, we can look for a_{10} next to the

x^{10}. If we want to look for the total number of subsets that have a sum divisible by 5, we can look for the sum

$$S = a_0 + a_5 + a_{10} + a_{15} + \ldots + a_{N-5}x^{N-5} + a_N x^N$$

It would be nice if we can find a number z such that $z^{5k} = 1$ for all $k \in \mathbb{N}$ and $z^n =$ something else for $n \neq 5k$. This way, we can isolate all the a_{5k} s and be closer to finding out the answer.

If we know about complex numbers, we will find that the complex number

$$z = \cos(72°) + \mathbf{i}\sin(72°)$$

satisfies the equation $z^5 = 1$, thus also satisfies $z^{5k} = 1$ for all $k \in \mathbb{N}$.

For those not familiar of complex numbers, this result follows from the **De Moivre's formula** [35] (see next 3 pages for proof), which states that

$$(r(\cos\theta + \mathbf{i}\sin\theta))^n = r^n(\cos n\theta + \mathbf{i}\sin n\theta)$$

where r is a real number. If we substitute $r = 1$, $\theta = 72°$, $n = 5$, we get

$$(\cos 72° + \mathbf{i}\sin 72°)^5 = \cos 5(72°) + \mathbf{i}\sin 5(72°) = 1$$

Also note that $z^n = z^{n+5k}$ for all $n \in \{0, 1, 2, 3, 4\}, k \in \mathbb{N}$. This means that the power of z is a cycle of z^0, z^1, z^2, z^3, z^4, .

If we plug z^0, z^1, z^2, z^3, z^4 into the generating function $A(x)$ respectively:

$$\begin{aligned}
A(z^0) &= a_0 + a_1z^0 + a_2z^0 + a_3z^0 + \ldots + a_Nz^0\\
A(z^1) &= a_0 + a_1z^1 + a_2z^2 + a_3z^3 + \ldots + a_Nz^N\\
A(z^2) &= a_0 + a_1z^2 + a_2z^4 + a_3z^6 + \ldots + a_Nz^{2N}\\
A(z^3) &= a_0 + a_1z^3 + a_2z^6 + a_3z^9 + \ldots + a_Nz^{3N}\\
A(z^4) &= a_0 + a_1z^4 + a_2z^8 + a_3z^{12} + \ldots + a_Nz^{4N}
\end{aligned}$$

Adding the five equations together (please zoom in):

$$\begin{aligned}
&A(z^0) + A(z^1) + A(z^2) + A(z^3) + A(z^4)\\
=&5a_0 + a_5(z^0 + z^5 + z^{10} + z^{15} + z^{20}) + a_{10}(z^0 + z^{10} + z^{20} + z^{30} + z^{40}) + \ldots + a_N(z^0 + z^N + z^{2N} + z^{3N} + z^{4N})\\
&+ a_1(z^0 + z^1 + z^2 + z^3 + z^4) + a_6(z^0 + z^6 + z^{12} + z^{18} + z^{24}) + \ldots + a_{N-4}(z^0 + z^{N-4} + z^{2(N-4)} + z^{3(N-4)} + z^{4(N-4)})\\
&+ a_2(z^0 + z^2 + z^4 + z^6 + z^8) + a_7(z^0 + +z^7 + z^{14} + z^{21} + z^{28}) + \ldots + a_{N-3}(z^0 + z^{N-3} + z^{2(N-3)} + z^{3(N-3)} + z^{4(N-3)})\\
&+ a_3(z^0 + z^3 + z^6 + z^9 + z^{12}) + a_8(z^0 + z^8 + z^{16} + z^{24} + z^{32}) + \ldots + a_{N-2}(z^0 + z^{N-2} + z^{2(N-2)} + z^{3(N-2)} + z^{4(N-2)})\\
&+ a_4(z^0 + z^4 + z^8 + z^{12} + z^{16}) + a_9(z^0 + z^9 + z^{18} + z^{27} + z^{36}) + \ldots + a_{N-1}(z^0 + z^{N-1} + z^{2(N-1)} + z^{3(N-1)} + z^{4(N-1)})
\end{aligned}$$

Note that $z^0 + z^{5k} + z^{10k} + z^{15k} + z^{20k} = 5$ for all $k \in \mathbb{N}$, and

$$z^0 + z^n + z^{2n} + z^{3n} + z^{4n} = z^0 + z^1 + z^2 + z^3 + z^4$$

for all n not divisible by 5. This is because for all n not divisible by 5,

$$\{n, 2n, 3n, 4n\} \equiv \{1, 2, 3, 4\} \pmod 5 \qquad \ldots(*)$$

In other words, each of the first 4 multiples of a natural number is congruent (mod 5) to each of 1, 2, 3, 4 shuffled in some other. This fact follows from what I call the 'clock theorem', and the proof is there 2.10.1.

Since addition is commutative, how the terms are shuffled won't change the whole sum. Thus,

$$\begin{aligned} z^0 + z^n + z^{2n} + z^{3n} + z^{4n} &= z^0 + z^{5k_1+1} + z^{5k_2+2} + z^{5k_3+3} + z^{5k_4+4} \\ &= z^0 + z^1 + z^2 + z^3 + z^4 \\ &= \frac{z^5 - 1}{z - 1} \qquad \text{(finite geometric series formula)} \\ &= 0 \end{aligned}$$

which means

$$A(z^0) + A(z^1) + A(z^2) + A(z^3) + A(z^4) = 5S$$

$$S = \frac{1}{5}(A(z^0) + A(z^1) + A(z^2) + A(z^3) + A(z^4)) \qquad \ldots(**)$$

Let's consider the factored form of $A(z)$. Because of the cyclic nature of z^n (i.e. $z^{5k+n} = z^n$),

$$\begin{aligned} A(z) &= (1+z)(1+z^2)(1+z^3)(1+z^4)(1+z^5)\ldots(1+z^{2000}) \\ &= ((1+z)(1+z^2)(1+z^3)(1+z^4)(1+z^5))^{400} \end{aligned}$$

How do we evaluate $(1+z)(1+z^2)(1+z^3)(1+z^4)(1+z^5)$? We need not use a calculator actually. First, consider the equation $x^5 - 1 = 0$. The complex roots of this equation are z^1, z^2, z^3, z^4, z^5. This means the equation can also be written in the factored form

$$(x - z)(x - z^2)(x - z^3)(x - z^4)(x - z^5) = 0$$

Thus,

$$x^5 - 1 \equiv (x - z)(x - z^2)(x - z^3)(x - z^4)(x - z^5)$$

Putting $x = -1$,

$$(-1)^5 - 1 = (-1-z)(-1-z^2)(-1-z^3)(-1-z^4)(-1-z^5)$$

$$(1+z)(1+z^2)(1+z^3)(1+z^4)(1+z^5) = 2$$

Nice. We got what we desired to get. So

$$A(z) = ((1+z)(1+z^2)(1+z^3)(1+z^4)(1+z^5))^{400} = 2^{400}$$

Using similar reasoning,

$$\begin{aligned} A(z^2) &= ((1+z^2)(1+z^4)(1+z^6)(1+z^8)(1+z^{10}))^{400} \\ &= ((1+z)(1+z^2)(1+z^3)(1+z^4)(1+z^5))^{400} \qquad \text{(shuffled)} \\ &= 2^{400} \end{aligned}$$

And also, $A(z^3) = A(z^4) = 2^{400}$

Finally, since $z^0 = 1$,

$$A(z^0) = \underbrace{(1+z^0)(1+z^0)(1+z^0)\dots(1+z^0)}_{\text{2000 times}} = 2^{2000}$$

Recall the equation (**). Now that the values are all known, we can evaluate S:

$$\begin{aligned} S =& \frac{1}{5}(2^{2000} + 2^{400} + 2^{400} + 2^{400} + 2^{400}) \\ =& 229626139054850904846566640235536396804463540417739040095528 \\ & 547365153252278474062771331897263301253983689192927797492554 \\ & 689423792172611066285186271233330637078259978290624560001377 \\ & 558296480089742857853980126972489563230927292776727894634052 \\ & 080932707941809993116324797617889259211246623299072328443940 \\ & 665362688337817968917011204758969615828117801869553000858005 \\ & 433413251661044016264472562583522535766634413197990792836254 \\ & 043559716808084319706366503081778867804183841109915567179344 \\ & 098978162939128529882758114227191547025694343915472652211663 \\ & 105403892946226485600614638808511782738582394749745484278005 \\ & 76 \end{aligned}$$

So the required probability is:

$P(X \text{ is divisible by } 5)$

$= \dfrac{S}{2^{2000}}$

$= \dfrac{\frac{1}{5}(2^{1598}+1)}{2^{1598}}$

$=$

$$\boxed{\frac{2223120823854702231000840703275868215790961725606891965970911154687684153488457611949239128808698470874297676057052469187255352822764198965819250835080640505978129253931020798836535284917254351951796538063754191363270279803270908682634251789444905699581352116462342515701493858081124370593888978944604851484523076600095765568343123447107444610299894191413286064514811012460133737033490735290928238250498015019482092166096800420823688757225596462339412327976948547864808031318232269}{111156041192735111550042035163793410789548086280344598298545557734384207674422880597461956440434923543714883802852623459362767641138209948290962541754032025298906462696551039941826764245862717597589826903187709568163513990163545434131712589472245284979067605823117125785074692904056218529694448947230242574226153830004788278417156172355372230514994709570664303225740550623006686851674536764546411912524900750974104608304840021041184437861279823116970616398847427393240401565911613 44}}$$

Proof of De Moivre's formula

We will use mathematical induction. We have the preposition

$$(r(\cos\theta + \mathbf{i}\sin\theta))^n = r^n(\cos n\theta + \mathbf{i}\sin n\theta)$$

. When $n = 1$, LHS $= (r(\cos\theta + \mathbf{i}\sin\theta))^1 = r^1(\cos 1\theta + \mathbf{i}\sin 1\theta) =$ RHS

$\therefore$ The statement is true for $n = 1$.

Assume the statement is true for some positive integer k. Then

$$(r(\cos\theta + \mathbf{i}\sin\theta))^k = r^k(\cos k\theta + \mathbf{i}\sin k\theta)$$

When $n = k + 1$,

$$\begin{aligned}
\text{LHS} &= (r(\cos\theta + \mathbf{i}\sin\theta))^k(r(\cos\theta + \mathbf{i}\sin\theta)) \\
&= r^k(\cos k\theta + \mathbf{i}\sin k\theta)(r(\cos\theta + \mathbf{i}\sin\theta)) \qquad \text{(induction hypothesis)} \\
&= r^{k+1}(\cos k\theta\cos\theta + \mathbf{i}\cos k\theta\sin\theta + \mathbf{i}\sin k\theta\cos\theta - \sin k\theta\sin\theta) \\
&= r^{k+1}(\cos k\theta\cos\theta - \sin k\theta\sin\theta + \mathbf{i}(\cos k\theta\sin\theta + \sin k\theta\cos\theta)) \\
&= r^{k+1}(\cos(k\theta + \theta) + \mathbf{i}\sin(k\theta + \theta)) \qquad \text{(compound angle formula)} \\
&= r^{k+1}(\cos(k+1)\theta + \mathbf{i}\sin(k+1)\theta) \\
&= \text{RHS}
\end{aligned}$$

$\therefore$ The statement is true for $n = k + 1$.

By mathematical induction, the statement $(r(\cos\theta+\mathbf{i}\sin\theta))^n = r^n(\cos n\theta+\mathbf{i}\sin n\theta)$ is true for all positive integers n. □

For the proof of the 'clock theorem', it involves some number theory concepts explained in the previous section (Section 1.4)

Here's the 'clock theorem'. ('Clock' because modular arithmetic kind of works like a clock.)

Preposition. If there are two positive integers a, n which are coprime (i.e. gcd(a, n)=1) , then

$$\{0, a, 2a, \ldots, (n-1)a\} \equiv \{0, 1, 2, \ldots, n-1\} \pmod n$$

Explanation

Let A denote the set $\{0, a, 2a, \ldots, (n-1)a\}$ and $\mathbb{Z}_n$ denote the set $\{0, 1, 2, \ldots, n-1\}$. If we take mod n for each element in A, the new set will be the same as $\mathbb{Z}_n$. The elements are shuffled in some way in the new set but sets do not account for order, so we can still list the new elements inside the set $\mathbb{Z}_n$ in ascending order.

Mathematically, the theorem says that function $f : A \to \mathbb{Z}_n$ for which $f(x) = x \,\%\, n$ is a **bijective** function (meaning there is a one-to-one correspondence for the elements of the two sets with nothing left over). An equivalent statement is that $\{i \,\%\, n \,|\, i \in A\} = \mathbb{Z}_n$.

("$\{i \,\%\, n \,|\, i \in A\}$" uses the set builder notation and means the set of all elements in A (mod n).)

Another interpretation is that if there is a clock with n numbers on it (from 0 to $n-1$), and I start from 0 and skip (clockwise) around the clock a

numbers each step. After $n-1$ steps, I must have visited every number on the clock exactly once (including the starting point).

Let's move on to the actual proof.

Proof of 'clock theorem' [36]

For any integer a, let $a' = a \% n$, and so $a' = \mathbb{Z}_n$. Thus, for any positive integer k,

$$(ak) \% n = ((a \% n)k) \% n = (a'k) \% n \qquad \text{(remainder proeprty)}$$

. That means, the set of values obtained for a and a' are exactly the same.

Thus, for the purpose of our proof we can assume $a \in \mathbb{Z}_n$, and the theorem will stand proved for any integer a.

Let a, n be comprime integers (gcd(a,n)=1). Let t be the least positive integer such that $(at) \% n = 0$. That is,

$$n \Dashv at \quad \Leftrightarrow \quad at \text{ is a multiple of } n$$

Let m be a positive integer such that $nm = at$. But this is a positive common multiple of a and n. Since we are looking for the value of t:

$$\begin{aligned} at &= \operatorname{lcm}(a, n) \\ &= \frac{an}{\gcd(a, n)} && \text{(property of product of LCM and GCD)} \\ &= an \\ t &= n \end{aligned}$$

That means an is the least integer that can be divided by n.

Now, consider all $i \in \mathbb{Z}_n$, i.e. $i = 0, 1, 2, \ldots, n{-}1$. Suppose for some $i_1, i_2 \in \mathbb{Z}_n$ with $i_1 < i_2$, we have

$$(ai_1) \% n = (ai_2) \% n \qquad \Longleftrightarrow \qquad (a(i_2 - i_1)) \% n = 0$$

. Let $d = i_2{-}i_1$. So, $(ad) \% n = 0$. But $0 < i_2{-}i_1 < n$. So, $0 < d < n$, which is impossible since n is the least positive integer with $(an) \% n = 0$.

Hence, for any $i_1, i_2 \in \mathbb{Z}_n$, if $i_1 \neq i_2$, then $(ai_1) \% n \neq (ai_2) \% n$.

In other words, for all $i \in \mathbb{Z}_n$, the values of $(ai) \% n$ are distinct, but we also have $0 \leq ((ai) \% n) \leq n$. The n elements in $\{0, a, 2a, \ldots, (n-1)a\}$ map to $\{0, 1, 2, \ldots, n-1\}$ distinctly (a bijection) when taking mod n, which means

$$\{0, a, 2a, \ldots, (n-1)a\} \equiv \{0, 1, 2, \ldots, n-1\} \pmod{n}$$

□

There is another much shorter solution for the puzzling puzzle, and this is too good to not share:

Solution 67b. (Copied from [37]) (Answer of how to find S)

> “ We're asking how many subsets of $[1, 2, 3, 4, 0, 1, 2, 3, 4, 0, ...4, 0]$ add to 0 mod 5.
>
> This is 2^{400} times the number of subsets of $[1, 2, 3, 4, 1, 2, 3, 4, ...2, 3, 4]$ that do so.
>
> The answer is invariant under shuffling, so we can instead think of subsets of $[1, 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, ...]$.
>
> But this equivalent mod 5 to $[1, 2, 4, 8, 16, ...]$. So we're just counting the number of integers between 0 and $2^{1600} - 1$ which are multiples of 5, as seen by writing them in binary.
>
> So the answer is $2^{400} \times \left\lceil \frac{2^{1600}}{5} \right\rceil$. ”
>
> The above expression is equivalent to $\frac{1}{5}(2^{2000} + 4(2^{100}))$.
>
> The remaining steps to find the required probability is the same as Solution a, so I will not write it again.

Discussion 67b. This is certainly a classy solution, using only 5 sentences to explain the answer (as opposed to the 5 page solution using generating functions). But that doesn't mean that the solution using generation function is useless. It means that even the less intelligent person can also arrive at the solution using a more complicated method (?) .

2.10.2 Using generating functions to solve for recursive formulas

When we want to find the general solution to a recursive formula, sometimes we may use generating functions to help us.

Ordinary generation function

Recall the sequence b_n from the second solution of the last problem of section 2.8.2 , defined by the recursive formula $b_n = b_{n-1} + 2b_{n-2}$ with initial condition $b_1 = 1$, $b_2 = 3$. Using generation function to solve for the general formula of b_n is much more complicated than using the method in section 2.8.2 , but worth writing about nonetheless, as it familiarizes us with this method.

For convenience's sake, let $b_0 = 1$ (which is consistent with the recursive formula). Define $B(x) = \sum_{n \geq 1} b_n x^n = b_1 x + b_2 x^2 + b_3 x^3 + \dots$.

Multiplying both sides by x^n in the recursive formula (with shifted index):

$$b_{n+1}x^n = b_n x^n + 2b_{n-1}x^n$$

Substituting values for all $n \geq 1$:

$$\begin{gathered} b_2 x^1 = b_1 x^1 + 2b_0 x^1 \\ b_3 x^2 = b_2 x^2 + 2b_1 x^2 \\ b_4 x^3 = b_3 x^3 + 2b_2 x^3 \\ \vdots \end{gathered}$$

Summing up all the equations, we have:

$$\sum_{n \geq 1} b_{n+1} x^n = \sum_{n \geq 1} b_n x^n + 2 \sum_{n \geq 1} b_{n-1} x^n$$

$$\begin{aligned} \frac{B(x) - b_1 x}{x} &= B(x) + 2x(B(x) + b_0) \\ B(x) - (1)x &= xB(x) + 2x^2 B(x) + (1)(2x^2) \\ B(x)(1 - x - 2x^2) &= x + 2x^2 \\ B(x) &= \frac{x + 2x^2}{1 - x - 2x^2} \\ &= (x + 2x^2) \cdot \frac{1}{(1 - 2x)(1 + x)} \end{aligned}$$

Note that the factorization $1 - x - 2x^2 \equiv (1 - 2x)(1 + x)$ can be found by setting $1 - x - 2x^2 \equiv (1 + mx)(1 + nx) \equiv 1 + (m + n)x + mnx^2$. We have $m + n = -1$ and $mn = -2$. Solving (without loss of generality), $m = 1$ and $n = -2$.

Using **partial fraction decomposition** [13] on $\dfrac{1}{(1 - 2x)(1 + x)}$:

$$\frac{1}{(1 - 2x)(1 + x)} \equiv \frac{A}{1 - 2x} + \frac{B}{1 + x}$$

[13] Partial fraction decomposition decomposes the fraction $\frac{f(x)}{p(x)q(x)}$ into the sum $\frac{A}{p(x)} + \frac{B}{q(x)} + C$ where A, B, C are constants. It is the reverse operation of "summing two fractions together by finding their common denominator".

Multiply both sides by $(1-2x)(1+x)$:

$$1 \equiv A(1+x) + B(1-2x)$$

Since this is an **identity** [14] , we can substitute some easy values for x in order to find A, such as $\frac{1}{2}$:

$$\begin{aligned} 1 &\equiv A(1+\frac{1}{2}) + B(1-2(\frac{1}{2})) \\ A &= \frac{2}{3} \end{aligned}$$

Similar to find B , substitute $x=-1$ to make the A term become 0:

$$\begin{aligned} 1 &\equiv A(1+(-1)) + B(1-2(-1)) \\ B &= \frac{1}{3} \end{aligned}$$

Thus,

$$B(x) = \frac{(x+2x^2)}{3} \cdot (\frac{2}{(1-2x)} + \frac{1}{(1+x)})$$

Note that $\dfrac{1}{1-r} = 1 + r + r^2 + r^3 + \ldots$ for $|r| < 1$ by the geometric series formula. So (we can pretend that $B(x)$ is defined for $-1 < x < 1$):

$$\begin{aligned} B(x) &= \frac{(x+2x^2)}{3} \cdot \big((2 + 2(2x) + 2(2x)^2 + 2(2x)^3 + \ldots) + (1 + (-x) + (-x)^2 + (-x)^3 + \ldots)\big) \\ &= \frac{(x+2x^2)}{3} \cdot \big((2-1) + (2^2 + (-1))x + (2^3 + (-1)^2)x^2 + (2^4 + (-1)^3)x^3 + \ldots\big) \\ &= \frac{(x+2x^2)}{3} \cdot \sum_{n \geq 0} (2^{n+1} + (-1)^n)x^n \\ &= \frac{1}{3}\left[x\sum_{n \geq 0}(2^{n+1} + (-1)^n)x^n + 2x^2\sum_{n \geq 0}(2^{n+1} + (-1)^n)x^n\right] \\ &= \frac{1}{3}\left[\sum_{n \geq 0}(2^{n+1} + (-1)^n)x^{n+1} + 2\sum_{n \geq 0}(2^{n+1} + (-1)^n)x^{n+2}\right] \\ &= \frac{1}{3}\left[\sum_{n \geq 1}(2^{n} + (-1)^{n-1})x^{n} + 2\sum_{n \geq 2}(2^{n-1} + (-1)^n)x^{n}\right] \end{aligned}$$

[14] An identity with variable x holds true for all values of x , which means the LHS and RHS are equal no matter what value of x is substituted.

Since $(2^0 + (-1)^1) = 0$,

$$\sum_{n\geq 2}(2^{n-1} + (-1)^n)x^n = \sum_{n\geq 1}(2^{n-1} + (-1)^n)x^n$$

.

$$\begin{aligned}
B(x) &= \frac{1}{3}\left[\sum_{n\geq 1}(2^n + (-1)^{n-1})x^n + 2\sum_{n\geq 1}(2^{n-1} + (-1)^n)x^n\right] \\
&= \frac{1}{3}\sum_{n\geq 1}\left[\,(2^n + (-1)^{n-1}) + 2(2^{n-1} + (-1)^n)\,\right]x^n \\
&= \frac{1}{3}\sum_{n\geq 1}\left[\,2(2^n) + 2(-1)^n - (-1)^n)\,\right]x^n \\
\sum_{n\geq 1} b_n x^n &= \sum_{n\geq 1}\frac{2^{n+1} + (-1)^n}{3}\,x^n
\end{aligned}$$

Thus , $b_n = \dfrac{2^{n+1} + (-1)^n}{3}$.

It is interesting how a function that does nothing but encode a sequence as the constants of a polynomial can magically spit out the general formula for us , and we never substituted x for any actual values (except the partial fraction decomposition, in which substitution of x is also not necessary anyway).

Exponential generating function

Exponential generating function is in the form $A(x) = \sum_{n\geq 0} = a_n\dfrac{x^n}{n!}$. It is usually used for something permutation-related, such as finding the general formula from the recursive formula of derangements.

Recall the recursive formula of derangement numbers:

$$D_n = (n+1)(D_{n-1} + D_{n-2})$$

with initial conditions $D_0 = 1$ and $D_1 = 0$. For convenience, let $D_{-1} = 0$, which is consistent with the recurrence. Multiply both sides by $\dfrac{x^n}{n!}$ in the formula (with shifted index): [38]

$$\begin{aligned} D_{n+1}\frac{x^n}{n!} &= n(D_n + D_{n-1})\frac{x^n}{n!} \\ D_{n+1}\frac{x^n}{n!} &= nD_n\frac{x^n}{n!} + nD_{n-1}\frac{x^n}{n!} \end{aligned}$$

Substituting values for all $n \geq 0$:

$$\begin{aligned} D_1\frac{x^0}{0!} &= 0D_0\frac{x^0}{0!} + 0D_{-1}\frac{x^0}{0!} \\ D_2\frac{x^1}{1!} &= 1D_1\frac{x^1}{1!} + 1D_0\frac{x^1}{1!} \\ D_3\frac{x^2}{2!} &= 2D_2\frac{x^2}{2!} + 2D_1\frac{x^2}{2!} \\ &\vdots \end{aligned}$$

Summing up all the equations:

$$\sum_{n\geq 0} D_{n+1}\frac{x^n}{n!} = \sum_{n\geq 0} nD_n\frac{x^n}{n!} + \sum_{n\geq 0} nD_{n-1}\frac{x^n}{n!} \tag{1}$$

Let

$$D(x) = \sum_{n\geq 0} D_n\frac{x^n}{n!}$$

be the exponential generating function in question. Then take the **derivative** [15] of the function:

$$D'(x) = \sum_{n\geq 0} nD_n\frac{x^{n-1}}{n!} = \sum_{n\geq 1} nD_n\frac{x^{n-1}}{n!} = \sum_{n\geq 1} D_n\frac{x^{n-1}}{(n-1)!} = \sum_{n\geq 0} D_{n+1}\frac{x^n}{n!} \tag{2}$$

$$xD'(x) = x\sum_{n\geq 0} nD_n\frac{x^{n-1}}{n!} = \sum_{n\geq 0} nD_n\frac{x^n}{n!} \tag{3}$$

[15] In calculus, the derivative of a function is the rate of change or the slope of the function. The derivative of $f(x)$, denoted $f'(x)$, is defined by the **first principle**:
$f'(x) = \lim_{h\to 0}\frac{f(x+h)-f(x)}{h}$.
The act of taking the derivative is also called **differentiation**.

and

$$xD(x) = \sum_{n\geq 0} D_n \frac{x^{n+1}}{n!} = \sum_{n\geq 0}(n+1)D_n \frac{x^{n+1}}{(n+1)!} = \sum_{n\geq 1} nD_{n-1}\frac{x^n}{n!} = \sum_{n\geq 0} nD_{n-1}\frac{x^n}{n!} \tag{4}$$

since $D_{-1} = 0$. Putting (2), (3), (4) into (1):

$$D'(x) = xD'(x) + xD(x)$$

$$(1-x)D'(x) = xD(x)$$

This is a separable **differential equation** :

$$\frac{D'(x)}{D(x)} = \frac{x}{1-x}$$

Let $y = D(x)$. Then $\frac{dy}{dx} = D'(x)$. Using separation of variables to **integrate** [16] both sides (It works but I don't know why. I should probably learn more Calculus):

$$\begin{aligned} \frac{\frac{dy}{dx}}{y} &= \frac{x}{1-x} \\ \frac{dy}{y} &= \frac{x}{1-x}dx \\ \int \frac{dy}{y} &= \int \frac{x}{1-x}dx \end{aligned}$$

[16] Integration is the reverse operation of differentiation, and $\int f'(x)dx = f(x) + C$ for some constant C .

Use **u-substitution** on RHS. Let $x = u + 1$. Then $dx = du$.

$$
\begin{aligned}
\int \frac{dy}{y} &= \int \frac{u+1}{1-(u+1)} du \\
\ln(y) &= -\int \frac{u+1}{u} du \\
\ln(y) &= -\int (1 + \frac{1}{u}) du \\
\ln(y) &= -(u + \ln|u|) + C \\
\ln(y) &= -x - \ln|x-1| + C \\
y &= e^{-x - \ln|x-1| + C} \\
y &= \frac{e^{-x} e^{C}}{e^{\ln|x-1|}} \\
D(x) &= \frac{Ce^{-x}}{|1-x|}
\end{aligned}
$$

(C is an 'absorbing constant' because we don't care about its value yet.) Assume that $|x| < 1$. Then expanding e^{-x} and $\dfrac{1}{1-x}$:

$$
\begin{aligned}
D(x) &= C(1 + x + x^2 + x^3 + \ldots)(\frac{1}{0!} - \frac{1}{1!}x + \frac{1}{2!}x^2 - \frac{1}{3!}x^3 + \frac{1}{4!}x^4 - \ldots) \\
\sum_{n \geq 0} D_n \frac{x^n}{n!} &= C(\frac{1}{0!} + (\frac{1}{0!} - \frac{1}{1!})x + (\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!})x^2 + (\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!})x^3 + \ldots) \\
\sum_{n \geq 0} D_n x^n &= \sum_{n \geq 0} (Cn! \sum_{k=0}^{n} \frac{(-1)^k}{k!})
\end{aligned}
$$

Since $D_0 = 1$, we have $C = 1$ and $D_n = n! \sum_{k=0}^{n} \dfrac{(-1)^k}{k!}$.

Interestingly, using generating function to convert the recursive formula into the general formula doesn't need to use the inclusion-exclusion principle, so generation functions can sometimes serve as an alternative path to arrive at the same destination.

Let's see if the general formula of a_n back in the solution of the last problem of 2.8.2 can be solved in a similar way. (I wasted too much time pondering how to find that general formula.)

We have the recursive formula

$$
a_n = 2n\, a_{n-1} + 8n(n-1)a_{n-2}
$$

with initial condition $a_0 = 1$ and $a_1 = 2$. For convenience, let $a_{-1} = 0$ which is consistent with the recursive formula. Multiply both sides by $\frac{x^n}{n!}$ (with shifted index):

$$\begin{aligned} a_{n+1}\frac{x^n}{n!} &= 2(n+1)a_n\frac{x^n}{n!} + 8(n+1)na_{n-1}\frac{x^n}{n!} \\ a_1\frac{x^0}{0!} &= 2(1)a_0\frac{x^0}{0!} + 8(1)(0)a_{-1}\frac{x^0}{0!} \\ a_2\frac{x^1}{1!} &= 2(2)a_1\frac{x^1}{1!} + 8(2)(1)a_0\frac{x^1}{1!} \\ a_3\frac{x^2}{2!} &= 2(3)a_2\frac{x^2}{2!} + 8(3)(2)a_1\frac{x^2}{2!} \\ &\vdots \end{aligned}$$

Summing up the equations over all $n \geq 0$:

$$\sum_{n\geq 0} a_{n+1}\frac{x^n}{n!} = 2\sum_{n\geq 0}(n+1)a_n\frac{x^n}{n!} + 8\sum_{n\geq 0}(n+1)na_{n-1}\frac{x^n}{n!} \tag{1}$$

Let $A(x) = \sum_{n\geq 0} a_n\frac{x^n}{n!}$. Then with the experience of solving the previous recursive formula, we know that

$$xA'(x) = x\sum_{n\geq 0} na_n\frac{x^{n-1}}{n!} = \sum_{n\geq 0} na_n\frac{x^n}{n!} \tag{2}$$

$$A'(x) = \sum_{n\geq 1} na_n\frac{x^{n-1}}{n!} = \sum_{n\geq 1} a_n\frac{x^{n-1}}{(n-1)!} = \sum_{n\geq 0} a_{n+1}\frac{x^n}{n!} \tag{3}$$

and

$$xA(x) = \sum_{n\geq 0}(n+1)a_n\frac{x^{n+1}}{(n+1)!} = \sum_{n\geq 1} na_{n-1}\frac{x^n}{n!} = \sum_{n\geq 0} na_{n-1}\frac{x^n}{n!} \tag{4}$$

$$A'(x) = \sum_{n\geq 0} na_n\frac{x^{n-1}}{n!} = \sum_{n\geq 1}(n-1)a_{n-1}\frac{x^{n-2}}{(n-1)!} = \sum_{n\geq 0} n(n-1)a_{n-1}\frac{x^{n-2}}{n!}$$

$$\begin{aligned} x^2A'(x) &= \sum_{n\geq 0} n(n-1)a_{n-1}\frac{x^n}{n!} \\ &= \sum_{n\geq 0} n^2a_{n-1}\frac{x^n}{n!} - \sum_{n\geq 0} na_{n-1}\frac{x^n}{n!} \end{aligned}$$

Put (4) into the rightmost sum:

$$x^2A'(x) = \sum_{n\geq 0} n^2 a_{n-1}\frac{x^n}{n!} - xA(x)$$

$$x^2A'(x) + xA(x) = \sum_{n\geq 0} n^2 a_{n-1}\frac{x^n}{n!} \tag{5}$$

Recall (1):

$$\begin{aligned}\sum_{n\geq 0} a_{n+1}\frac{x^n}{n!} &= 2\sum_{n\geq 0}(n+1)a_n\frac{x^n}{n!} + 8\sum_{n\geq 0}(n+1)na_{n-1}\frac{x^n}{n!} \\ &= 2(\sum_{n\geq 0} na_n\frac{x^n}{n!} + \sum_{n\geq 0} a_n\frac{x^n}{n!}) + 8(\sum_{n\geq 0} n^2a_{n-1}\frac{x^n}{n!} + \sum_{n\geq 0} na_{n-1}\frac{x^n}{n!})\end{aligned}$$

Put (3), (2), (4), (5) into the above equation:

$$A'(x) = 2(xA'(x) + A(x)) + 8(x^2A'(x) + xA(x) + xA(x))$$

$$\begin{aligned}A'(x)(1-2x-8x^2) &= A(x)(16x+2) \\ \frac{A'(x)}{A(x)} &= \frac{16x+2}{1-2x-8x^2}\end{aligned}$$

Let $y = A(x)$. Then $\frac{dy}{dx} = A'(x)$.

$$\begin{aligned}\frac{\frac{dy}{dx}}{y} &= \frac{16x+2}{1-2x-8x^2} \\ \int\frac{dy}{y} &= \int\frac{16x+2}{-(8x^2+2x-1)}dx \\ \ln(y) &= -\ln|8x^2+2x-1| + C \\ y &= \frac{C}{1-2x-8x^2} = C(\frac{1}{(1+2x)(1-4x)})\end{aligned}$$

Taking partial fraction of $\frac{1}{(1+2x)(1-4x)}$:

$$1 \equiv A(1-4x) + B(1+2x)$$

$$A = \frac{1}{3} \quad \text{and} \quad B = \frac{2}{3}$$

So

$$
\begin{aligned}
y &= \frac{C}{3}(\frac{1}{1+2x} + \frac{2}{1-4x}) \\
A(x) &= \frac{C}{3}(1 + (-2x) + (-2x)^2 + (-2x)^3 + \ldots + 2 + 2(4x) + 2(4x)^2 + 2(4x)^3 + \ldots) \\
A(x) &= \frac{C}{3}((2+1) + (2^3 + (-2)^1)x + (2^5 + (-2)^2)x^2 + (2^7 + (-2)^3)x^3 + \ldots) \\
\sum_{n \geq 0} a_n \frac{x^n}{n!} &= \frac{C}{3} \sum_{n \geq 0} (2^{2n+1} + (-2)^n)x^n \\
\sum_{n \geq 0} a_n x^n &= C \sum_{n \geq 0} \frac{(2^{n+1} + (-1)^n)2^n n!}{3} x^n
\end{aligned}
$$

Since $a_0 = 1$ and $\frac{(2^1+(-1)^0)2^0 0!}{3} = 1$, we have $C = 1$ and $a_n = \dfrac{(2^{n+1} + (-1)^n)2^n n!}{3}$
.

What a ride. Now we finally know how to derive this general formula legitimately instead of helplessly staring at it and hoping the solution will come up by itself. All thanks to the trusty exponential generating function.

2.11 Partition of integers / Putting identical balls into identical boxes

Partition of integer has come up briefly in the problems in section 2.7.3 to help us find distinct formations of multiple dice. The number of distinct partitions of an integer (without regard to order among the parts) is called the partition number, denoted $p(n)$. For example, $p(5) = 7$, with the partitions listed below:

$$
\begin{aligned}
5 &= 5 \\
&= 4 + 1 \\
&= 3 + 1 + 1 \\
&= 3 + 2 \\
&= 2 + 1 + 1 + 1 \\
&= 2 + 2 + 1 \\
&= 1 + 1 + 1 + 1 + 1
\end{aligned}
$$

The partition numbers themselves are rarely the direct answer to a probability problem, but we can use them to check if we have listed out all the possibilities in some problems, so it is still a topic of interest.

2.11.1 Recursive formula

[39]

Let $p(n, k)$ be the number of partitions of integer n that have parts that are all not larger than k. For example, $p(7, 4) = 11$, as

$$\begin{aligned}
7 &= 4 + 3 \\
&= 4 + 2 + 1 \\
&= 4 + 1 + 1 + 1 \\
&= 3 + 3 + 1 \\
&= 3 + 2 + 2 \\
&= 3 + 2 + 1 + 1 \\
&= 3 + 1 + 1 + 1 + 1 \\
&= 2 + 2 + 2 + 1 \\
&= 2 + 2 + 1 + 1 + 1 \\
&= 2 + 1 + 1 + 1 + 1 + 1 \\
&= 1 + 1 + 1 + 1 + 1 + 1 + 1
\end{aligned}$$

Note that all the partitions of $p(7, 3)$ appear in the partitions of $p(7, 4)$ that do not include '4' as a part. This is not a coincidence, as when we are using parts up to 4 in the partition of integer 7, we must include the parts up to 3 somewhere in the list too.

The rest of the partitions that are not in $p(7, 3)$ but in $p(7, 4)$ must include '4' as a part, and we can freely partition the remaining integer '3' , which has $p(3, 4)$ partitions in total. Thus, $p(7, 4) = p(7, 3) + p(3, 4)$.

In general, we have $p(n, k) = p(n, k - 1) + p(n - k, k)$.

Note that $p(n, n) = p(n)$, and when $n < k$, $p(n, k) = p(n, n) = p(n)$, because there is no way we can partition an integer into a part larger than itself.

Now we take a look at the base cases. When $n = 0$, we consider partitioning nothing as the only way to partition the integer 0 , so $p(0, k) = 1$ for all $k \geq 0$. When $n > 0$ and $k = 0$, there are no way to partition a positive integer n using only '0's , so $p(n, 0) = 0$. If $n < 0$, we don't consider partitioning negative integers to be valid, so $p(n, k) = 0$. If $k < 0$, it is impossible to happen in the recursive formula anyway, so we can ignore it (or make it undefined).

Thus, we can define the two-argument partition function recursively as follows:

$$p(n,k) = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } k = 0 \text{ or } n < 0 \\ p(n,k-1) + p(n-k,k) & \text{otherwise} \end{cases}$$

The python recursive implementation of this is:

```
def p(n,k):
    if n == 0:
        return 1
    elif k == 0 or n < 0:
        return 0
    else:
        return p(n, k-1) + p(n-k, k)
```

This is a good starting point, but the problem is that recursion is often too inefficient in codes , and it would take forever to calculate for larger inputs like $p(100, 100)$. Fortunately there is a more efficient implementation using **dynamic programming**.

First we initialize with an $(n + 1) \times (k + 1)$ array (/list) all containing 0 (the +1 is because we count starting from 0). The goal is to let the element in the n th row and k th column represent $p(n, k)$ (count starting from 0). We make all the elements in the 0 th row to be 1 , and also make all the elements in the 0 th column (except $p(0, 0)$) to be 0 (actually they are already 0).

Then starting from top to bottom (in the order we write stuff) , we make all the 0 in the j th row and i th column (except the 0 th column) to be the sum of two parts: (i) the element in $i - 1$ th column and same row , and (ii) the element in the $j - i$ th row and same column. If the position of element is out of bounds, just take it to be 0. The python code implementation of this process is:

```
def p(n,k):
    arr = []
    for i in range(n+1):
        arr.append( [0] * (k+1))
    for i in range(k+1):
        arr[0][i] = 1
    for j in range(1, n+1):
        for i in range(1, k+1):
            if j-i >= 0:
                arr[j][i] = arr[j-i][i] + arr[j][i-1]
            else:
                arr[j][i] = arr[j][i-1]
    return arr, f'partitions: {arr[-1][-1]}'
```

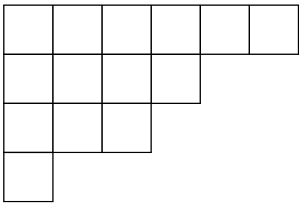
This returns a 2d array of $p(j, i)$ for $0 \leq j \leq n$ and $0 \leq i \leq k$. For example, to find $p(10, 7)$, we get

```
([[1, 1, 1, 1, 1, 1, 1, 1],
  [0, 1, 1, 1, 1, 1, 1, 1],
  [0, 1, 2, 2, 2, 2, 2, 2],
  [0, 1, 2, 3, 3, 3, 3, 3],
  [0, 1, 3, 4, 5, 5, 5, 5],
  [0, 1, 3, 5, 6, 7, 7, 7],
  [0, 1, 4, 7, 9, 10, 11, 11],
  [0, 1, 4, 8, 11, 13, 14, 15],
  [0, 1, 5, 10, 15, 18, 20, 21],
  [0, 1, 5, 12, 18, 23, 26, 28],
  [0, 1, 6, 14, 23, 30, 35, 38]],
 'partitions: 38')
```

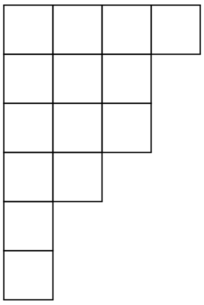
So $p(10, 7) = 38$.

2.11.2 Young diagram

We can represent a partition with a **Young diagram** , which is made of a bunch of squares. For example, the partition $6 + 4 + 3 + 1$ of the integer 14 can expressed by the following diagram:

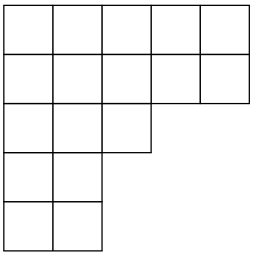


Each row consists of a part, and the number of squares in the row is the size of that part. Now if we reflect the diagram diagonally (meaning the axis of reflection is a diagonal line starting from the top left corner) , we get:



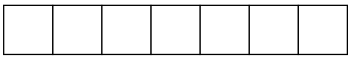
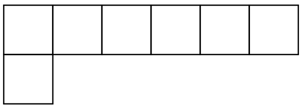
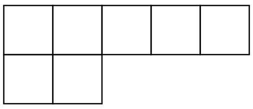
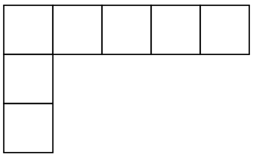
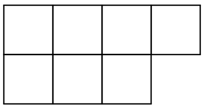
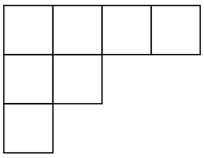
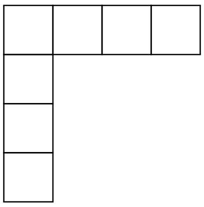
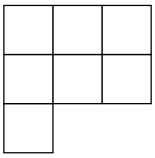
This represents a different partition of 14 , which is 4+3+3+2+1+1 . This new partition is called the **conjugate** of the original partiton $6 + 4 + 3 + 1$. Note that every partition has a unique conjugate, and no two distinct partitions share the same conjugate.

A partition can be the conjugate of itself, such as $5 + 5 + 3 + 2 + 2$:



Let's list the 15 partitions of the integer 7 in Young diagrams and conjugates pairs: (next page)

(Since a partition's conjugate's conjugate is the partition itself, it is sufficient to list the diagrams for only half of the partitions.)

Partition	Young diagram	Conjugate
7		$1+1+1+1+1+1+1$
$6+1$		$2+1+1+1+1+1$
$5+2$		$2+2+1+1+1$
$5+1+1$		$3+1+1+1+1$
$4+3$		$2+2+2+1$
$4+2+1$		$3+2+1+1$
$4+1+1+1$		$4+1+1+1$
$3+3+1$		$3+2+2$

Note that the size of the largest part of a partition is the number of parts of its conjugate. We see that the maximum size of parts and the number of parts form a bijection over the conjugate pairs. Note that $4+1+1+1$ is the only the only self-conjugate.

Let $q(n, k)$ be the number of partitions of integer n that have not more than k parts. When $p(n, k)$ counts a partition with maximum part size of m (or 'includes' it in the partition list), $q(n, k)$ must also count that partition's conjugate because the conjugate has m parts too. When $q(n,k)$ counts a partition with l parts, $p(n,k)$ must also count its conjugate because the conjugate's maximum part size is l too.

Let P_n be the set containing all the partitions of integer n , and let $f : P_n \to P_n$ be a bijective function that maps every partition to its conjugate. Let $P_{n,k}$ be the subset of P_n that contains all the partitions with parts not larger than k . Then the set of images of $P_{n,k}$, denoted $f[P_{n,k}]$, must be the set of all partitions with not more than k parts (because of our observation in the diagrams above), and since bijection preserve set size, we must have $|P_{n,k}| = |f[P_{n,k}]|$, and $p(n,k) = q(n,k)$.

Balls into boxes

Another interpretation of the partition of integer n is putting n identical balls into n identical boxes, in which some boxes can be left empty. Each box represents a part and the number of balls in a box represents the size of the part. For example, for the partition $7 = 3 + 2 + 2$, there would be 3 balls in the first box, 2 balls in the second box, and 2 balls in the third box. The rest of the boxes are empty. (Since we regard the boxes as identical, any arrangement of the boxes is consider the same, so we can default the boxes to be arranged in descending number of balls contained.)

Thus, the number of ways to put 7 identical balls into 7 identical boxes is $p(7) = 15$,and in general, the number of ways to put n identical balls into n identical boxes is $p(n)$.

What about putting n identical balls into k identical boxes where $k \leq n$? In this case, we are just limiting the number of parts used in the partition to be not more than k, and we have shown that the number of ways to do this is the same as the number of ways to partition the integer using parts not larger than k , which is $p(n,k)$.

So the number of ways to put n identical balls into k identical boxes is $p(n,k)$.

2.11.3 Generating function of partition

Is there a nice general formula for the partition number (or partition function) $p(n)$? Unfortunately there is not, but let's see what we can do with it.

Let $P(x) = \sum_{n\geq 0} p(n)x^n$ be the generating function of the partition numbers. To choose a partition of the number n , first we can choose the number of '1's to be included in the partition, then choose the number of '2's to be included , then '3', and so on. We can express this as a polynomial:

$$P(x) = (1+x+x^2+x^3+\ldots)(1+x^2+x^4+x^6+\ldots)\cdots(1+x^i+x^{2i}+x^{3i}+\ldots)\cdots$$

Using geometric series formula on each factor, we get

$$P(x) = (\frac{1}{1-x})(\frac{1}{1-x^2})(\frac{1}{1-x^3})(\frac{1}{1-x^4})\cdots$$

$$P(x) = \prod_{n=1}^{\infty}(\frac{1}{1-x^n})$$

If we want to find all the partition numbers up to $p(n)$, then we can just multiply out all the terms with degree not more than n and discard the rest. For example, to find $p(0)$ to $p(8)$, we expand the partial product

$$(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8)(1+x^2+x^4+x^6+x^8)(1+x^3+x^6)$$
$$(1+x^4+x^8)(1+x^5)(1+x^6)(1+x^7)(1+x^8)$$
$$= 1+x+2x^2+3x^3+5x^4+7x^5+11x^6+15x^7+22x^8+\ldots+x^{56}$$

The terms with degree higher than 8 can be discarded since they are not accurate. We see that $p(8) = 22$, $p(7) = 15$, $p(6) = 11$, and so on.

To find $p(i, k)$ for i from 0 to n with fixed k , we can further chop off (truncate) the product after the k th factor. For example, to find $p(8, 4)$, we expand the partial product

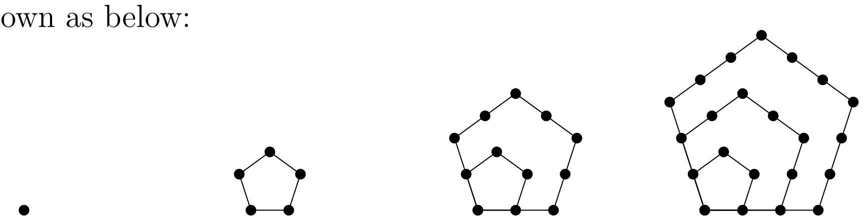
$$(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8)(1+x^2+x^4+x^6+x^8)$$
$$(1+x^3+x^6)(1+x^4+x^8)$$
$$= 1+x+2x^2+3x^3+5x^4+6x^5+9x^6+11x^7+15x^8+\text{whatever}$$

We see that $p(8, 4) = 15$, $p(7, 4) = 11$, $p(6, 4) = 9$ and so on.

2.11.4 Euler's pentagonal number theorem

Euler's pentagonal number theorem gives a recursive formula that allows us to calculate $p(n)$ for large n much more quickly than the previous dynamic programming method , like $p(50000)$. (Don't ask me why I need to know what $p(50000)$ is.)

First let me introduce the **pentagonal numbers** . Let $g(n)$ denote the n th pentagonal number. Then $g(n) = \frac{n(3n-1)}{2}$. It counts the number of nodes of a bunch of pentagons of different sizes sharing the same corner, shown as below:



$n = 1$ $n = 2$ $n = 3$ $n = 4$

Now let's get to the actual theorem.

Preposition.

$$\prod_{n=1}^{\infty}(1-x^n) = 1+\sum_{k=1}^{\infty}(-1)^k(x^{k(3k-1)/2}+x^{k(3k+1)/2})$$

$$(1-x)(1-x^2)(1-x^3)\cdots = 1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-\ldots$$

Proof. First, we consider counting partitions with non-repeating parts. For example, $9 =$ 2+3+4 is a non-repeating partition. Let $Q(x)$ be the generating function for the number of non-repeating partition of n . To choose a non-repeating partition, first we choose whether '1' is a part or not, then choose whether '2' is a part or not, then '3' , and so on. So

$$Q(x) = (1$$

□

3 Countably infinite outcomes, events and trials

So far, we have been mainly talking about finite outcomes in the sample space, or finite events or trials, but as we saw in Problem 41.1, sometimes there can be countably infinite trials, such as throwing a dice until it lands on '3'. The possible number of throws ranges from 1 to infinity, and each of the throw can be labelled with a natural number with no unlabelled throws left over.

Since we do not care about the exact sequence of the numbers thrown, except whether a '3' occurs for the first time, we can simply each dice throw to a Bernoulli trial with only two outcomes: success (getting a '3') or failure (not getting a '3'). Once a success is achieved, the sequence of trials is terminated. The possible sequences of outcomes of the trials is 'S' or 'FS' or 'FFS' or 'FFFS' or 'FFFFS' and so on. If all of trials conducted are viewed as an experiment as a whole, then this experiment's possible outcomes are the possible sequences of outcomes of each individual trials, which are countably infinite.

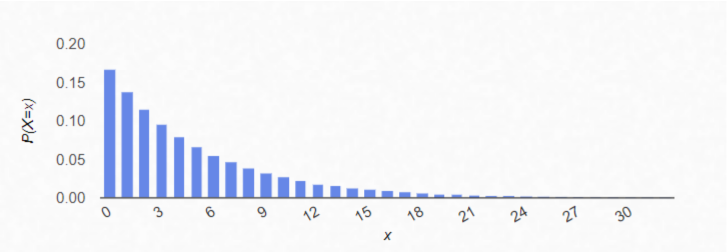
Working with infinite outcomes or infinite events is similar to finite outcomes or events, and the probability rules such as addition rule, multiplication rule, complement rule, independent events means independent complements, distributive laws, DeMorgan's laws, law of total probability all hold as usual. The only difference is one is finite and one is countably infinite.

3.1 Geometric distribution

Let X be the number of dice throws required to get the number '3' for the first time. Then $P(X=1)=\frac{1}{6}$. If more than one throw is required for '3' to appear, then the first throw must be a number other than '3', which has a $\frac{5}{6}$ probability of occurring. Given that the 1st throw is not a '3', the probability that the 2nd throw is a '3' is $\frac{1}{6}$. So $P(X=2)=(\frac{5}{6})(\frac{1}{6})$. By similar reasoning, $P(X=3)=(\frac{5}{6})^2(\frac{1}{6})$, $P(X=4)=(\frac{5}{6})^3(\frac{1}{6})$, and so on.

In general, the probability that n throws is required to get the number '3' for the first time is $P(X=n)=(\dfrac{5}{6})^{n-1}(\dfrac{1}{6})$. The probability distribution of X follows the **geometric distribution**, as there is a common ratio between every $P(X=n)$ and $P(X=n+1)$.

The bar graph of the probability distribution of X is:



We can see that the sum of the probabilities of all values of X is

$$\begin{aligned} & P(X=1)+P(X=2)+P(X=3)+\ldots \\ &= \frac{1}{6}+(\frac{5}{6})(\frac{1}{6})+(\frac{5}{6})^n(\frac{1}{6})+\ldots \\ &= \frac{\frac{1}{6}}{1-(\frac{5}{6})} \qquad \text{(geometric series formula)} \\ &= 1 \end{aligned}$$

So it makes sense. This method can be generalized to any Bernoulli trials. We have the formula for geometric distribution:

Theorem 3.1. If in a Bernoulli trial, the probability of getting a success is p , and the probability of getting a failure is $1-p$, then the probability of getting a success for the first time in the n th trial is

$$P(n)=p\,(1-p)^{n-1}$$

If we want to find the probability of getting the first success in not more than n trials, then the required probability is

$$\begin{aligned} P(\leq n) &= 1-P(>n) \\ &= 1-(1-p)^n \end{aligned}$$

Note that this is also equivalent to the probability of getting at least one success in n trials.

Problem 68. I repeatedly throw five dice at the same time (each throw of five dice counts as one throw), until I get at least three '6's in the same throw. What is the probability that I stop throwing after less than 10 throws? (Express the answer as a percentage cor. to 2 d.p.)

(Difficulty level: 7)

Solution 68. Let p be the probability of getting at least three '6's in the same throw.

$$\begin{aligned} p &= P(\text{three '6'}) + P(\text{four '6'}) + P(\text{five '6'}) \\ &= C_3^5(\frac{5}{6})^2(\frac{1}{6})^3 + C_4^5(\frac{5}{6})(\frac{1}{6})^4 + C_5^5(\frac{1}{6})^5 \\ &= \frac{23}{648} \end{aligned}$$

Let X be the number of dice throws required to get at least three '6's.

$$\begin{aligned} \text{Required probability} &= P(1 \leq X \leq 9) \\ &= 1 - P(X > 10) \\ &= 1 - (1 - \frac{23}{648})^{10} \\ &= \boxed{30.33\%} \end{aligned}$$

3.2 Pascal distribution

Return to the one dice situation again. What if I won't stop throwing the dice until I get exactly k number '6's? Let n be the total number of throws required to get exactly k number '6's. Then the n th throw must be a '6', since I immediately stop throwing after getting k number '6's. In the first $n-1$ throws, $k-1$ number '6's have occurred. Using the binomial formula, the probability that '6' occurs $k-1$ times in $n-1$ throws is

$$C_{k-1}^{n-1}\,(\frac{1}{6})^{k-1}\,(\frac{5}{6})^{(n-1)-(k-1)} = C_{k-1}^{n-1}\,(\frac{1}{6})^{k-1}\,(\frac{5}{6})^{n-k}$$

Thus, the probability that n throws are required is the above expression times p. The total number of throws n follows the **Pascal distribution**. This can be generalized to any Bernoulli trials. We have the formula for Pascal distribution:

Theorem 3.2. If in a Bernoulli trial, the probability of getting a success is $\frac{1}{6}$, and the probability of getting a failure is $1-p$, then the probability that the k th success occurs in the n th trial is (for $0 < k \leq n$):

$$P(n) = C_{k-1}^{n-1}\,p^k\,(1-p)^{n-k}$$

If we want to find the probability of getting the first k successes in not more than n trials, then the required probability is

$$P(\leq n) = \sum_{r=k}^{n} C_{k-1}^{r-1} p^k (1-p)^{r-k}$$

Note that this is also equivalent to the probability of getting at least k successes in n trials.

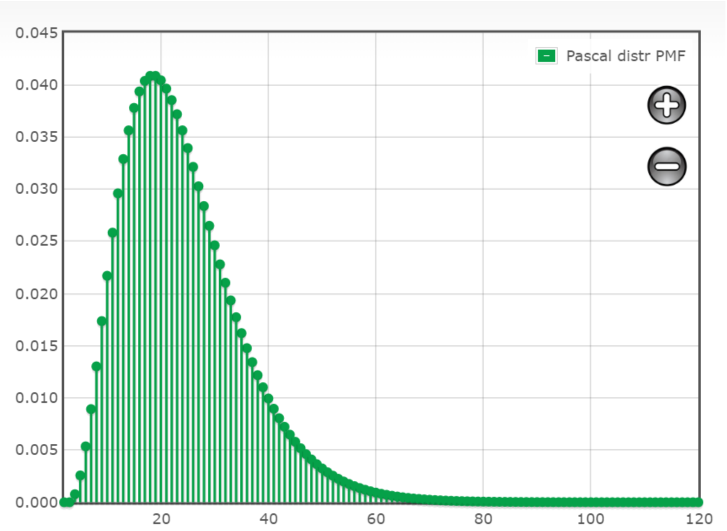
Problem 69. I throw a dice repeatedly until exactly 4 number '6' occurs. What is the probability that less than 25 throws are required? (Express the answer as a percentage cor. to 2 d. p.)

(Difficulty level: 7)

Solution 69. It is more convenient to first find the probability that 25 or more throws are required. For this to happen, the number of '6' obtained in the first 24 throws can be 0, 1, 2 or 3. Using the binomial formula,

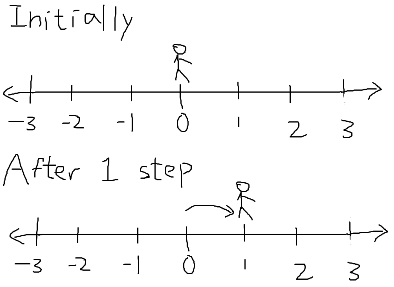
$$\begin{aligned} P(25 \text{ and more throws}) &= \sum_{r=0}^{3} C_r^{24} (\frac{1}{6})^r (\frac{5}{6})^{24-r} \\ &\approx 41.55\% \\ P(\text{less than 25 throws}) &\approx 1 - 41.55 \approx \boxed{58.45\%} \end{aligned}$$

Discussion 69. Here is a graph of the probability distribution of the number of dice throws.



3.3 1-dimensional random walk

Imagine that we want to get k successes in some Bernoulli trials, but it comes with a twist: Every failure will undo a success by decreasing the success count by 1. The success count may even go to negative values. This is called a **random walk**, as it is equivalent to randomly walking 1 unit left or 1 unit right on the integer number line (denoted by $\mathbb{Z}$) starting from 0 (can also be other integers), and trying to reach integer k. Since we can only go in two directions: left and right, we call it a 1-dimensional random walk.



Each step, we can move 1 unit right or 1 unit left. Moving 1 unit right can be expressed as ‘+1’ , and moving 1 unit left can be expressed as ‘-1’ . So the sequence of steps can be (+1, +1, -1, +1, -1, …). It keeps going until the sum of the sequence reaches k , and then terminates. We define the possible outcomes to be the possible integers that the pointer (or the person) lands on (called the destination) after a finite number of steps , but the number of steps can tend to infinity, just like the number of dice throws in a geometric distribution.

Let us show that that the random walk has countably infinite possible outcomes by showing that every possible sequence can be mapped to a natural number. Assume that the sequence does not terminate after reaching k. Label ‘+1’ as a success (S), and ‘-1’ as a failure (F). After 0 step, the sequence is empty ‘’ . After 1 step, there are 2 possible sequence of steps: ‘S’ and ‘F’. After 2 steps, there are $2^2 = 4$ possible sequences: ‘SS’, ‘SF’, ‘FS’, ‘FF’ . After i steps, there are 2^i possible sequences. Even if each of the possible sequences leads to a different integer as the destination (which is not actually the case, but I am assuming it for the sake of argument), we can assign the empty sequence ‘’ to 1, the sequence ‘S’ to 2 and ‘F’ to 3. Then assign the four 2-step sequences to 4, 5, 6, 7 respectively. Then we assign the eight 3-step sequences to integers from 8 to 15. In general, we assign all the 2^i i-step sequences to integers from 2^i to $2^{i+1} - 1$. This way, every sequence can be labelled with a distinct integer. Since the actual number of possible outcomes is less than that, the actual possible outcomes can be mapped to natural numbers as well.

3.3.1 Gambler's ruin

Let's first consider a random walk problem with one desired destination and one undesired destination.

Problem 70. Alice and Bob are playing a game. Each player starts with 12 tokens, and in each turn, three dice are rolled at the same time. If the sum of the numbers obtained is 14, Alice gets a token from Bob. If the sum of the numbers obtained is 11 instead, Bob gets a token from Alice. Otherwise, nobody gives or gets a token. The loser of the game is the first to reach zero tokens. What is the ratio of the probability that Alice wins the game to the probability that Bob wins the game?

(Difficulty level: 9) [2] (Classic Problems of Probability Q5 Modified)

Discussion 70. We are not prepared for this at all. We will get back to this later...

(Copied from this paper) [40]

First, let's simplify the situation to only one gambler who starts with an initial fortune of \$$a$. On each successive gamble, they either gain \$1 or lose \$1 independent of the past with probabilities p and $q = 1{-}p$ respectively. The gambler's objective is to reach a total fortune of \$$N$, without first getting *ruined* (he has zero money). If the gambler succeeds, then the gambler is said to *win* the game. In any case, the gambler stops playing after winning or getting ruined, whichever happens first.

Let P_i denote the probability that the gambler wins the game when they have \$$i$. By definition, $P_N = 1$ and $P_0 = 0$. If the gambler has \$$i$, then they will gain \$1 with probability p, and when they have \$$i + 1$, they will win the game with P_{i+1}. Similarly, when the gambler has \$$i$, they will lose \$1 with probability q, and then they will win the game with probability P_{i-1} . So we have

$$P_i = pP_{i-1} + qP_{i-1} \tag{1}$$

Since $p + q = 1$, equation (1) can be rewritten as $pP_i + qP_i = pP_{i-1} + qP_{i-1}$, yielding

$$P_{i+1} - P_i = \frac{q}{p}(P_i - P_{i-1})$$

In particular, $P_2 - P_1 = \frac{q}{p}(P_1 - P_0) = \frac{q}{p}P_1$ (since $P_0 = 0$), so that $P_3 - P_2 = \frac{q}{p}(P_2 - P_1) = (\frac{q}{p})^2 P_1$, and more generally

$$P_{i+1} - P_i = (\frac{q}{p})^i P_1 \quad (0 < i < N)$$

Thus,

$$\begin{aligned} P_{i+1} - P_1 &= P_{i+1} - P_i + P_i - P_{i-1} + P_{i-1} - \ldots - P_2 + P_2 - P_1 \\ &= \sum_{r=1}^{i}(P_{r+1} - P_r) \\ &= \sum_{r=1}^{i}(\frac{q}{p})^r P_1 \end{aligned}$$

yielding

$$\begin{aligned} P_{i+1} &= P_1 + P_1 \sum_{r=1}^{i}(\frac{q}{p})^r \\ &= P_1 \sum_{r=0}^{i}(\frac{q}{p})^r \\ &= \begin{cases} P_1 \dfrac{1-(\frac{q}{p})^{i+1}}{1-\frac{q}{p}}, & \text{if } p \neq q \\ P_1(i+1), & \text{if } p = q = \frac{1}{2} \end{cases} \end{aligned} \tag{2}$$

(For the $p \neq q$ case, we are using the "finite geometric series" equation $\sum_{i=0}^{n-1} ar^i = a\,\frac{1-r^n}{1-r}$, where a is the first term, r ($\neq 1$) is the common ratio, and n is the number of terms. See the next page for the derivation of the formula.)

Choosing $i = N{-}1$ and using the fact that $P_N = 1$ yields

$$1 = P_N = \begin{cases} P_1 \dfrac{1-(\frac{q}{p})^{N}}{1-\frac{q}{p}}, & \text{if } p \neq q \\ P_1 N, & \text{if } p = q = \frac{1}{2} \end{cases}$$

from which we conclude that (make P_1 the subject for both cases):

$$P_1 = \begin{cases} \dfrac{1-\frac{q}{p}}{1-(\frac{q}{p})^{N}}, & \text{if } p \neq q \\ \frac{1}{N}, & \text{if } p = q = \frac{1}{2} \end{cases}$$

thus obtaining from (2) (after algebra) the solution

$$P_i = \begin{cases} \dfrac{1-(\frac{q}{p})^i}{1-(\frac{q}{p})^N}, & \text{if } p \neq q \\ \frac{i}{N}, & \text{if } p = q = \frac{1}{2} \end{cases} \tag{3}$$

So if the gambler has an initial fortune of \$$a$, we can just substitute $i = a$ in equation (3) above. Now let's derive the geometric series formula.

Derivation of the finite geometric series formula

Let $S = a + ar + ar^2 + \ldots + ar^{n-1}$, where $r \neq 1$ and n is an integer larger than 0. Then

$$\begin{aligned} S &= a + ar + ar^2 + \ldots + ar^{n-1} \\ rS &= \quad\quad ar + ar^2 + ar^3 + \ldots + ar^n \\ rS - S &= ar^n - a \\ S(r-1) &= a(r^n - 1) \\ S &= a\,\frac{1-r^n}{1-r} \end{aligned} \qquad \square$$

Now we can return to Problem 70.

Problem 70. (Restated) Alice and Bob are playing a game. Each player starts with 12 tokens, and in each turn, three dice are rolled at the same time. If the sum of the numbers obtained is 14, Alice gets a token from Bob. If the sum of the numbers obtained is 11 instead, Bob gets a token from Alice. Otherwise, nobody gives or gets a token. The loser of the game is the first to reach zero tokens. What is the ratio of the probability that Alice wins the game to the probability that Bob wins the game?

(Difficulty level: 9)

Solution 70. First, we can use the formula $\sum_{r=0}^{n}(-1)^r\, C_r^n\, C_{n-1}^{k-rm-1}$ introduced in Theorem 2.12 to find the number of ways of getting a sum of 11 and a sum of 14 respectively in a dice throw.

Putting $m = 6$, $n = 3$, $k = 11$, we get:
Number of ways to get a sum of 11 $= C_2^{10} - C_1^3 C_2^4 = 27$
Number of ways to get a sum of 14 $= C_2^{13} - C_1^3 C_2^7 = 15$

We can ignore turns of the game in which the numbers of the dice sum to a number other than 11 or 14, since nothing will happen in those turns. So we are only interested in dice throws in which the sum is 11 or 14.

Given that the sum is 11 or 14, let p be the probability that the sum is 14 (in Alice's favour), and let q be the probability that the sum is 11 (in Bob's favour). Then $\dfrac{q}{p} = \dfrac{27}{15} = \dfrac{9}{5}$. Putting $i = 12$ and $N = 24$ in equation (3) above, we get

$$P(\text{Alice wins}) = \frac{1 - (\frac{9}{5})^{12}}{1 - (\frac{9}{5})^{24}} = \frac{244\,140\,625}{282\,673\,677\,106}$$

$$\text{Thus, } P(\text{Bob wins}) = 1 - \frac{244\,140\,625}{282\,673\,677\,106} = \frac{282\,429\,536\,481}{282\,673\,677\,106}$$

$$\text{Required ratio} = \frac{P(\text{Alice wins})}{P(\text{Bob wins})} = \boxed{\frac{244\,140\,625}{282\,429\,536\,481}}$$

Equation (3) can be generalized to any 1-d random walk problem.

Theorem 3.3. If a pointer on the integer number line starts at integer a, and at each step, walk 1 unit right (+1) with probability p, or walk 1 unit left (-1) with probability $q = 1 - p$, then the probability that the pointer reaches integer b before reaching 0 is:

$$P_{a,b} = \begin{cases} \dfrac{1 - (\frac{q}{p})^a}{1 - (\frac{q}{p})^b}, & \text{if } p \neq q \\ \frac{a}{b}, & \text{if } p = q = \frac{1}{2} \end{cases} \tag{4}$$

3.3.2 Becoming infinitely rich or getting ruined

What if there is only one desired destination, and no undesired destination? Or equivalently, what if there is only one undesired destination, and no desired destination?

If there are no desired destination, then we can take the limit when b tends to infinity. If $p > \frac{1}{2}$, then $\frac{q}{p} < 1$ and thus from equation (4):

$$\lim_{b\to\infty} P_{a,b} = 1 - (\frac{q}{p})^a > 0, \quad p > \frac{1}{2} \tag{5}$$

If $p \leq \frac{1}{2}$, then $\frac{q}{p} \geq 1$ and thus from equation (4):

$$\lim_{b\to\infty} P_{a,b} = 0, \quad p \leq \frac{1}{2} \tag{6}$$

To interpret the meaning of (5) and (6), suppose that the gambler starting with \$$a$ wishes to continue gambling forever until (if at all) ruined, with the intention of earning as much money as possible. So there is no winning value b; the gambler will only stop if ruined. What will happen? (5) says that if $p > \frac{1}{2}$ (each gamble is in his favor), then there is a positive probability that the gambler will never get ruined but instead will become infinitely rich. (6) says that if $p \leq \frac{1}{2}$ (each gamble is not in his favor), then with probability one the gambler will get ruined.

Problem 71. John is gambling and he starts with \$2. In each round, he will gain \$1 with probability 0.6, or lose \$1 with probability 0.4. If John never stops playing until he has zero dollars, what is the probability that John will become infinitely rich (the money he has never drops to 0) ?

(Difficulty level: 8) [40]

Solution 71. Using equation (5) above,

$$P(\text{infinitely rich}) = 1 - (\frac{1 - 0.6}{0.6})^2 = \boxed{\frac{5}{9}}.$$

3.4 Markov chains

Besides random walks on integer number lines, there are other types of random walks, like a random walk among a network of states. This network is called a **Markov chain**. [41]

3.4.1 Future probabilities

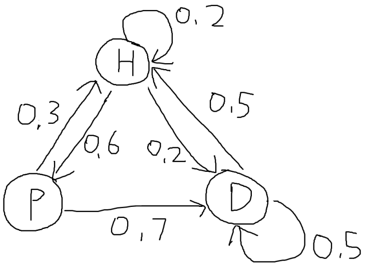
Suppose a restaurant sells only three types of food: hamburger (H), pizza (P) and hot dog (D). On any given day, they serve only one type of food, and it depends on what they have served yesterday. The probabilities of the food served is given by the following table:

Tomorrow Today	Hamburger	Pizza	Hot Dog
Hamburger	0.2	0.6	0.2
Pizza	0.3	0	0.7
Hot dog	0.5	0	0.5

If the restaurant serves hamburgers today, then it will sell hamburgers tomorrow with 0.2 probability, or pizzas tomorrow with 0.6 probability, or hot dogs tomorrow with 0.2 probability.

Similarly, if it sells pizza today, then it will sell hamburgers tomorrow with 0.3 probability, or hot dogs tomorrow with 0.7 probability. It will not sell pizzas tomorrow.

We can draw a **transition diagram** to represent this Markov chain:



The circles/ nodes in the graph are the **states** of the Markov chain, which are hamburger (H), pizza (P) and hot dog (D). The number beside the arrow is the **transition probability** from one state to another.

The food that the restaurant serves *tomorrow* only depends on what food it serves today, and does not depend on the past, such as the food sold yesterday (unlike the food served *today*), or 2 weeks ago. The restaurant is said to be **memory-less**. In other words, the probability of future actions are not dependent upon the steps that led up to the present state. This is the **Markov property** of Markov chains.

If the restaurant sells hamburgers today, what is the probability that it will sell hamburgers again 2 days later?

By referring to the graph or table above, we can find the probability of selling each type of food tomorrow, and then find the probability that it sells hamburgers the day after tomorrow, given that it sells a certain type of food tomorrow. Let t_0, t_1 and t_2 denote today, tomorrow, and the day after tomorrow (2 days later) respectively. We have

$$\begin{aligned} P(\text{H in } t_2) = &\quad P(\text{H in } t_1|\text{H in } t_0)\, P(\text{H in } t_2|\text{H in } t_1) \\ &+ P(\text{P in } t_1|\text{H in } t_0)\, P(\text{H in } t_2|\text{P in } t_1) \\ &+ P(\text{D in } t_1|\text{H in } t_0) P(\text{H in } t_2|\text{D in } t_1) \\ =&\, (0.2)(0.2) + (0.6)(0.3) + (0.2)(0.5) \\ =&\, 0.32 \end{aligned}$$

What if I want to find the probability that it sells hamburgers 10 days later given that it sells hamburgers today? The calculation is troublesome, and we need a systematic way to calculate the probabilities, or else we will lose track of what's going on.

Refer to the table above. We can encode the probabilities in a **matrix** [17] (preserving the order in the table):

$$A = \begin{bmatrix} 0.2 & 0.6 & 0.2 \\ 0.3 & 0 & 0.7 \\ 0.5 & 0 & 0.5 \end{bmatrix}$$

This matrix is called a **transition matrix**. We can also encode the food sold today (hamburger) in a row **vector** [18]: (Note: I am using row vector instead of column vector purely for typesetting convenience, and all the calculations onwards follow the row vector version instead of the conventional column vector version)

$$\vec{v_0} = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$$

This vector (called the state vector) represents the overall probabilities of selling each type of food (in the order of hamburger, pizza, hot dog) in a given day t. Let today be day 0, tomorrow be day 1, and so on. The state vector on day t is denoted $\vec{v_t}$. To get $\vec{v_1}$ (probabilities of food sold tomorrow), we multiply the vector by the transition matrix.

$$\begin{aligned} \vec{v_1} = \vec{v_0}A &= \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0.2 & 0.6 & 0.2 \\ 0.3 & 0 & 0.7 \\ 0.5 & 0 & 0.5 \end{bmatrix} \\ &= \begin{bmatrix} (1)(0.2)+(0)(0.3)+(0)(0.5) & (1)(0.6)+(0)(0)+(0)(0) & (1)(0.2)+(0)(0.7)+(0)(0.5) \end{bmatrix} \\ &= \begin{bmatrix} 0.2 & 0.6 & 0.2 \end{bmatrix} \end{aligned}$$

As you can see, each entry (number) of the vector $\vec{v_1}$ is the sum of three products. Each product consists of a number from the vector $\vec{v_0}$ and a number from the matrix A. For the 1st entry of $\vec{v_1}$, the numbers taken from $\vec{v_0}$ go from left of $\vec{v_0}$ to right of $\vec{v_0}$. At the same time, the numbers taken from the 1st column of A go from up to down. For the 2nd entry of $\vec{v_1}$, how the numbers are taken from $\vec{v_0}$ is the same as the 1st entry, but the numbers taken from A are in the 2nd column (up to down). Similarly, for the 3rd entry of $\vec{v_1}$, the numbers taken from A is the 3rd column (up to down). This is the gist of matrix multiplication.

[17] A matrix is a rectangular array or table of numbers arranged in rows and columns. It is typically used to solve systems of linear equations, or used to represent linear transformations in **linear algebra**.

[18] A vector is an object that has both magnitude (size) and direction. It can also multiply with a matrix to do stuff. In fact, vector is a special type of matrix that has only one column or one row. The former is called column vector and the latter is called row vector.

Now what about $\vec{v_2}$? Just multiply $\vec{v_1}$ by A again.

$$\begin{aligned}\vec{v_2} = \vec{v_1}A &= \begin{bmatrix}0.2 & 0.6 & 0.2\end{bmatrix}\begin{bmatrix}0.2 & 0.6 & 0.2\\ 0.3 & 0 & 0.7\\ 0.5 & 0 & 0.5\end{bmatrix}\\ &= \begin{bmatrix}0.32 & 0.12 & 0.56\end{bmatrix}\end{aligned}$$

We can see that the first entry of $\vec{v_2}$ is 0.32, which corresponds to the probability of selling hamburgers in day 2 (the day after tomorrow). We can also see the probabilities of selling pizzas or hot dogs in day 2.

In general, we have

$$\vec{v_t} = \vec{v_{t-1}}A \qquad \text{and} \qquad \vec{v_t} = \vec{v_0}A^t$$

Since matrix multiplication is associative, i.e. $(AB)C = A(BC)$, we can first raise a square matrix to the t th power by multiplying the matrix with itself. Multiplying two 3×3 matrices is similar to how we have multiplied the vector and matrix earlier. Just (comput regard the matrix in the left (the one to be multiplied) to be 3 row vectors stacked on top of each other. By letting the computer [42] do the calculation, we have

$$\vec{v_{10}} = \vec{v_0}A^{10} = \begin{bmatrix}0.352\,112\,157\,2 & 0.211\,294\,063\,2 & 0.436\,593\,779\,6\end{bmatrix}$$

So the probability that the restaurant sells hamburgers 10 days later given that it sells hamburgers today is about 0.352 .

If we keep going further, like to day 100:

$$\vec{v_{100}} = \vec{v_0}A^{100} = \begin{bmatrix}0.352\,112\,676\,1\ldots & 0.211\,267\,605\,6\ldots & 0.436\,619\,718\,3\ldots\end{bmatrix}$$

The probabilities of day 10 and day 100 are pretty close. It seems that the probabilities are converging to certain values, called the **equilibrium distribution**. If so, then for an infinitely large t, the input vector $\vec{v_t}$ should be exactly the same as the output vector $\vec{v_{t+1}}$. Let's set an equation and denote this special state vector by $\vec{v_E}$, which represents the equilibrium distribution. Maybe we can figure out the exact values the probabilities are converging to. (Note that in below, the sum of the entries in the vector is 1 because they are probabilities.)

$$\vec{v_E}A = \vec{v_E}$$

$$\begin{bmatrix} x & y & z \end{bmatrix} \begin{bmatrix} 0.2 & 0.6 & 0.2 \\ 0.3 & 0 & 0.7 \\ 0.5 & 0 & 0.5 \end{bmatrix} = \begin{bmatrix} x & y & z \end{bmatrix}$$

$$\begin{cases} 0.2x + 0.3y + 0.5z & = x \\ 0.6x & = y \\ 0.2x + 0.7y + 0.5z & = z \\ x + y + z & = 1 \end{cases}$$

Solving, we get $x = \frac{25}{71}$, $y = \frac{15}{71}$, $z = \frac{31}{71}$. Converting them to decimals and putting them into the vector:

$$\vec{v_E} = \begin{bmatrix} 0.352\,112\,676\,1 & 0.211\,267\,605\,6 & 0.436\,619\,718\,3 \end{bmatrix}$$

which is about the same as $\vec{v_{100}}$. So we confirmed that the probabilities are converging to these numbers. Interestingly, if the restaurant starts by selling pizzas or hot dogs on day 0, the probabilities will still converge to the same values. (I will spare the calculations here.) What that means is that in the long run (the restaurant operates until the end of time itself), hamburgers will have a ≈ 0.35 probability of being sold, or pizzas with ≈ 0.21 probability or hot dogs with ≈ 0.44 probability.

3.4.2 Convergence to equilibrium distribution

But why is there an equilibrium probability distribution for infinity large t? Well, there's a lot of explaining to do and you can skip this part if you don't care about it. (Skip to 3.4.6) First, let me introduce some concepts from linear algebra.

Vectors

A vector can be viewed as an arrow in the linear space/Euclidean space that has its tail on the origin and its head pointing to the coordinates represented by the entries. A vector has **magnitude** (/size/length) and **direction**. The ratio of the entries of a vector uniquely defines the direction of the vector. Two vectors are **parallel** if they have the same direction. For any two parallel vectors, the ratio of the entries in the two vectors are the same. For example, if there are two vectors

$$\vec{a} = \begin{bmatrix} a_1 & a_2 & a_3 \end{bmatrix} \qquad \text{and} \qquad \vec{b} = \begin{bmatrix} b_1 & b_2 & b_3 \end{bmatrix}$$

such that $a_1 : a_2 : a_3 = b_1 : b_2 : b_3$, then $\vec{a}$ and $\vec{b}$ are parallel.

The magnitude of vector $\vec{a}$ is $\sqrt{a_1^2 + a_2^2 + a_3^2}$. If all of the entries in the vector is scaled by a constant (scalar), the magnitude of the vector is scaled by this same constant.

Two vectors can be added together by adding their corresponding entries together. Geometrically, when vector $\vec{b}$'s tail is put onto the vector $\vec{a}$'s head, their sum $\vec{a} + \vec{b}$ is a vector that has its tail on $\vec{a}$'s tail and its head on $\vec{b}$'s head.

Let me call a vector that can be 'stretched' or 'squished' into any magnitudes a 'scalable vector'. A scalable vector has variable magnitudes but a fixed direction.

Scalars

A **scalar** is a constant that can be used to scale vectors to a different magnitude. A scalar can multiply with a vector, so that all of the entries in the vector is multiplied by that scalar. However, a scalar and a vector cannot be added together.

Linear combination [43]

If a vector $\mathbf{v}_1$ can be expressed as the sum of another two scalable vectors, $\mathbf{v}_2$ and $\mathbf{v}_3$, i.e.

$$\mathbf{v}_1 = a\mathbf{v}_2 + b\mathbf{v}_3$$

where a, b are scalars, then $\mathbf{v}_1$ is a **linear combination** of $\mathbf{v}_2$ and $\mathbf{v}_3$.

Linearly independent vectors

Two vectors are **linearly independent** if they are non-parallel. For three vectors, if the three vectors do not lie on the same plane or same line (/parallel) in 3-d space, they are linearly independent. Mathematically, if and only if $\mathbf{v}_1$, $\mathbf{v}_2$ $\mathbf{v}_3$ are linearly independent vectors, then the only scalars a, b, c that satisfy the equation

$$a\mathbf{v}_1 + b\mathbf{v}_2 + c\mathbf{v}_3 = \vec{0} \tag{1}$$

is $a = b = c = 0$. ($\vec{0}$ is the zero vector that has all of its entries being '0'.)

That means if there exists a, b, c that satisfy the equation, and any one of the a, b, c are non-zero scalars, then $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$ are not linearly independent (/are linearly dependent).

Another interpretation of linear independence is that any one vector cannot be expressed as a linear combination of the other two vectors. If there are some non-zero solution for scalars in the above equation above (say, $a \neq 0$), then we can move the two vectors, $\mathbf{v}_2$ and $\mathbf{v}_3$ to the other side of the equation and make $\mathbf{v}_1$ the subject, i.e.

$$\mathbf{v}_1 = -\frac{b}{a}\mathbf{v}_2 - \frac{c}{a}\mathbf{v}_3$$

which shows that $\mathbf{v}_1$ is the linear combination of $\mathbf{v}_2$ and $\mathbf{v}_3$.

Eigenvalues and eigenvectors

By the way, the equilibrium vector $\vec{v_E}$ is one of the **eigenvectors** of matrix A. An eigenvector (the row vector version) $\vec{v}$ of matrix A is a **non-zero** vector that satisfies the equation

$$\vec{v}A = \lambda\vec{v}$$

where λ is a scalar (constant) called **eigenvalue**. In our case, the vector $\vec{v_E}$ is associated with the eigenvalue 1. (More info about eigenvalues and eigenvectors at [44].)

There are two more eigenvalues of A but they are complex numbers. (An $n \times n$ matrix usually has n distinct eigenvalues.) Using a computer (we are gonna use that a lot), we find that they are $\frac{-\mathbf{i}\sqrt{39}-3}{20}$ and $\frac{\mathbf{i}\sqrt{39}-3}{20}$, where $\mathbf{i}$ is the imaginary unit ($\mathbf{i}^2 = -1$). Each eigenvalue (which is fixed) is associated with a scalable eigenvector. So for the three eigenvalues of A, there are three non-parallel eigenvectors that can take on any magnitudes. (For why the three eigenvectors are linearly independent, see [45].) Let $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$ denote the three eigenvectors of A (with specific magnitudes) respectively. Since $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$ are linearly independent, any arbitrary vector (with 3 entries) $\vec{v}$ can be expressed as the linear combination of the three eigenvectors (no matter what specific magnitudes the eigenvectors take on), namely

$$\vec{v} = a\,\mathbf{v}_1 + b\,\mathbf{v}_2 + c\,\mathbf{v}_3$$

where a, b, c are scalars.

Using eigenvalues to explain convergence

To explain why repeated multiplying the transition matrix A to the initial state vector $\vec{v_0} = [1, 0, 0]$ (or any other vectors whose sum of entries is 1) will converge to the eigenvector $\mathbf{v}_1$= $[\frac{25}{71}, \frac{15}{71}, \frac{31}{71}]$, first note that the sum of entries of the state vector is always 1, no matter how many times it is multiplied by A .

Let λ_1, λ_2, λ_3 denote the three eigenvalues of A respectively. By choosing some specific magnitudes of the eigenvectors $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$, the vector $\vec{v_0} =$

$[1, 0, 0]$ can be decomposed into the linear combination of the three eigenvectors, such that the scalars are λ_1, λ_2, λ_3:

$$\vec{v_0} = \lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \lambda_3\mathbf{v}_3 \qquad \ldots(*)$$

Using a computer to find the values (or you can calculate by hand if you are crazy enough.):

$$\begin{aligned}\vec{v_0} =&(1)\begin{bmatrix}\frac{25}{71} & \frac{15}{71} & \frac{31}{71}\end{bmatrix}\\ &+\left(\frac{-\mathbf{i}\sqrt{39}-3}{20}\right)\begin{bmatrix}-\frac{25}{142}+\frac{65\sqrt{39}}{426}\mathbf{i} & -\frac{385}{284}-\frac{45\sqrt{39}}{284}\mathbf{i} & \frac{435}{284}+\frac{5\sqrt{39}}{852}\mathbf{i}\end{bmatrix}\\ &+\left(\frac{\mathbf{i}\sqrt{39}-3}{20}\right)\begin{bmatrix}-\frac{25}{142}-\frac{65\sqrt{39}}{426}\mathbf{i} & -\frac{385}{284}+\frac{45\sqrt{39}}{284}\mathbf{i} & \frac{435}{284}-\frac{5\sqrt{39}}{852}\mathbf{i}\end{bmatrix}\end{aligned}$$

It is not necessary to find the exactly values of the entries of the vectors $\mathbf{v}_2$ and $\mathbf{v}_3$, but I am just finding them to showcase that it is possible.

Multiply by powered matrix A^t in both sides of (*):

$$\begin{aligned}\vec{v_0}A^t &= (\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \lambda_3\mathbf{v}_3)A^t\\ &= \lambda_1\mathbf{v}_1A^t + \lambda_2\mathbf{v}_2A^t + \lambda_3\mathbf{v}_3A^t \qquad \ldots(**)\end{aligned}$$

Recall that for an eigenvector $\vec{v}$, we have $\vec{v}A = \lambda\vec{v}$, which also means that $\vec{v}A^t = \lambda^t\vec{v}$. This is because if $\vec{v}A^k = \lambda^k\vec{v}$ is true for some k, then

$$\vec{v}A^{k+1} = \vec{v}A^kA = \lambda^k\vec{v}A = \lambda^k(\lambda\vec{v}) = \lambda^{k+1}\vec{v}$$

Thus, from (**) we continue:

$$\begin{aligned}\vec{v_0}A^t &= \lambda_1\mathbf{v}_1A^t + \lambda_2\mathbf{v}_2A^t + \lambda_3\mathbf{v}_3A^t\\ &= \lambda_1^{t+1}\mathbf{v}_1 + \lambda_2^{t+1}\mathbf{v}_2 + \lambda_3^{t+1}\mathbf{v}_3\\ &= (1)^{t+1}\mathbf{v}_1 + (\frac{-\mathbf{i}\sqrt{39}-3}{20})^{t+1}\mathbf{v}_2 + (\frac{\mathbf{i}\sqrt{39}-3}{20})^{t+1}\mathbf{v}_3 \qquad \ldots(***)\end{aligned}$$

The scalars are the only changing value as t increases. The powered complex scalars converge to 0 as $t \to \infty$, because their absolute values are smaller than 1.

For those not familiar with complex numbers, a complex number z in the form $a + b\mathbf{i}$ has an **absolute value** $r = \sqrt{a^2 + b^2}$. (The absolute value of

z is also denoted by $|z|$.) We can view a complex number as a 2-d vector in the complex plane, with absolute value as its magnitude.

For why a complex number with an absolute value smaller than 1 raised to a power of t converges to 0 as $t \to \infty$, first note that any complex number can be expressed in its **polar form** $r(\cos\theta + \mathbf{i}\sin\theta)$, where $\cos\theta = \frac{a}{r}$ and $\sin\theta = \frac{b}{r}$, and r is the absolute value. So a pair of r and θ corresponds to a unique complex number. Recall the **De Moivre's formula** [35]:

$$(r(\cos\theta + \mathbf{i}\sin\theta))^n = r^n(\cos(n\theta) + \mathbf{i}\sin(n\theta))$$

This formula is a consequence of the fact that when we multiply two complex numbers together, we multiply their absolute values to get the new r and add their angle θ to get the new θ. Thus, we have

$$\lim_{t\to\infty} \lambda_2^t = \lim_{t\to\infty} |\lambda_2|^t (\cos(t\theta) + \mathbf{i}\sin(t\theta))$$

$\lambda_2 = \frac{-\mathbf{i}\sqrt{39}-3}{20}$, and its absolute value is

$$|\lambda_2| = \sqrt{(-\frac{3}{20})^2 + (-\frac{\sqrt{39}}{20})^2} = \frac{3}{25} < 1$$

.

Since for $(\cos(t\theta) + \mathbf{i}\sin(t\theta))$, both the real part and imaginary part is bounded between -1 and 1 (inclusive), while $\lim_{t\to\infty} |\lambda_2|^t = 0$, we conclude that

$$\lim_{t\to\infty} |\lambda_2|^t (\cos(t\theta) + \mathbf{i}\sin(t\theta)) = 0$$

, which means $\lim_{t\to\infty} \lambda_2^t = 0$.

Similarly, for λ_3 , we have $\lim_{t\to\infty} \lambda_3^t = 0$. Thus,

$$\begin{aligned}
\lim_{t\to\infty} \vec{v_0}A^t &= \lim_{t\to\infty} \lambda_1^{t+1}\mathbf{v}_1 + \lim_{t\to\infty} \lambda_2^{t+1}\mathbf{v}_2 + \lim_{t\to\infty} \lambda_3^{t+1}\mathbf{v}_3 \\
&= \lim_{t\to\infty} (1)^{t+1}\mathbf{v}_1 + \lim_{t\to\infty} (\frac{-\mathbf{i}\sqrt{39}-3}{20})^{t+1}\mathbf{v}_2 + \lim_{t\to\infty} (\frac{\mathbf{i}\sqrt{39}-3}{20})^{t+1}\mathbf{v}_3 \\
&= \mathbf{v}_1 + 0\mathbf{v}_2 + 0\mathbf{v}_3 \\
&= \begin{bmatrix} \frac{25}{71} & \frac{15}{71} & \frac{31}{71} \end{bmatrix} \qquad \square
\end{aligned}$$

Since any arbitrary initial state vector $\vec{v_0}$ can be expressed as the linear combination of the three eigenvectors (with $\mathbf{v}_1$ fixed to $[\frac{25}{71}, \frac{15}{71}, \frac{31}{71}]$) , any initial probability distribution converges to $[\frac{25}{71}, \frac{15}{71}, \frac{31}{71}]$.

3.4.3 General formula for the power of matrix

Let's find out the general formula for A^t. But first, we need to introduce some terminology related to matrices.

Diagonal matrix

Generally, a matrix raised to a power is messy to calculate, but there is a special type of matrix that is easy to raise to a power, called a **diagonal matrix**, in which the entries outside the main diagonal are all zero. The main diagonal starts from the top left corner and ends at the bottom right corner. Usually, a diagonal matrix is a **square matrix** (i.e. with same number of rows and columns). An example of diagonal matrix is:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

Now multiply it by itself.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 2 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 1^2 & 0 & 0 \\ 0 & 5^2 & 0 \\ 0 & 0 & 2^2 \end{bmatrix}$$

Multiply it by itself again (3rd power).

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 2 \end{bmatrix}^3 = \begin{bmatrix} 1^2 & 0 & 0 \\ 0 & 5^2 & 0 \\ 0 & 0 & 2^2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 1^3 & 0 & 0 \\ 0 & 5^3 & 0 \\ 0 & 0 & 2^3 \end{bmatrix}$$

In general, we can see that

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 2 \end{bmatrix}^n = \begin{bmatrix} 1^n & 0 & 0 \\ 0 & 5^n & 0 \\ 0 & 0 & 2^n \end{bmatrix}$$

This property is true for any diagonal matrices. If we can somehow transform a regular matrix into a diagonal matrix, then we are golden.

Identity matrix

An **identity matrix** is a diagonal matrix (and also square matrix) with '1's on the main diagonal and '0's elsewhere. It is typically denoted by I. An example of identity matrix (of 3 × 3) is

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

We can see that an identity matrix I raised to any positive power is I itself. We can also see that any matrix M multiplied by I is M itself. We have:

$$MI = IM = M$$

Thus, we can view I as the matrix equivalent of the number '1'.

Inverse of a matrix

A square matrix M can have a unique inverse, denoted M^{-1}, such that their product is the identity matrix I. For all matrices M that have an inverse,

$$MM^{-1} = M^{-1}M = I$$

This is similar to how a real number a multiplied by its inverse a^{-1} is 1.

For example, if I have a matrix

$$M = \begin{bmatrix} -2 & 2 & -1 \\ 1 & -1 & 1 \\ 1 & 0 & 2 \end{bmatrix}$$

Then we can find an inverse of M (using a computer):

$$M^{-1} = \begin{bmatrix} -2 & -4 & 1 \\ -1 & -3 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

And we can verify that

$$MM^{-1} = \begin{bmatrix} -2 & 2 & -1 \\ 1 & -1 & 1 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} -2 & -4 & 1 \\ -1 & -3 & 1 \\ 1 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I$$

Diagonalization of matrix [46]

For matrix A, if there exists a diagonal matrix D and some matrix P such that

$$D = PAP^{-1} \tag{1}$$

Then we can raise both sides to a power n:

$$\begin{aligned} D^n &= (PAP^{-1})^n \\ D^n &= \underbrace{(PAP^{-1})(PAP^{-1})\dots(PAP^{-1})}_{n \text{ times}} \end{aligned}$$

All the $P^{-1}P$ s in the middle cancels out, which leaves us with

$$D^n = PA^nP^{-1}$$

which means

$$A^n = P^{-1}D^nP$$

How do we find this matrix P in the first place? Fortunately, the eigenvectors and eigenvalues are here to help.

Rewrite equation (1) as

$$PA = DP \tag{2}$$

This remotely resembles the equation $\vec{v}A = \lambda\vec{v}$, but with eigenvector $\vec{v}$ changed to P and eigenvalue λ changed to diagonal matrix D. Could it be that the P is made of eigenvectors?

For convenience, in $\mathbf{v}_1$, let's denote the 1st entry by $v_{1,1}$, 2nd entry of $\mathbf{v}_1$ by $v_{1,2}$, 3rd entry by $v_{1,3}$. So $\mathbf{v}_1 = [v_{1,1}, v_{1,2}, v_{1,3}]$. The other two eigenvectors are denoted similarly. Let's stack the eigenvectors $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$ together to create a matrix.

$$P = \begin{bmatrix} v_{1,1} & v_{1,2} & v_{1,3} \\ v_{2,1} & v_{2,2} & v_{2,3} \\ v_{3,1} & v_{3,2} & v_{3,3} \end{bmatrix}$$

Multiplying two 3×3 matrices is just like multiplying '3 row vectors stacked together' by a matrix. By the property of eigenvectors ($\vec{v}A = \lambda\vec{v}$):
(the fat round brackets denotes 'stacking')

$$\begin{aligned} PA = \begin{bmatrix} v_{1,1} & v_{1,2} & v_{1,3} \\ v_{2,1} & v_{2,2} & v_{2,3} \\ v_{3,1} & v_{3,2} & v_{3,3} \end{bmatrix} A &= \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{v}_3 \end{pmatrix} A \\ &= \begin{pmatrix} \mathbf{v}_1 A \\ \mathbf{v}_2 A \\ \mathbf{v}_3 A \end{pmatrix} = \begin{pmatrix} \lambda_1 \mathbf{v}_1 \\ \lambda_2 \mathbf{v}_2 \\ \lambda_3 \mathbf{v}_3 \end{pmatrix} \\ &= \begin{bmatrix} \lambda_1 v_{1,1} & \lambda_1 v_{1,2} & \lambda_1 v_{1,3} \\ \lambda_2 v_{2,1} & \lambda_2 v_{2,2} & \lambda_2 v_{2,3} \\ \lambda_3 v_{3,1} & \lambda_3 v_{3,2} & \lambda_3 v_{3,3} \end{bmatrix} \end{aligned}$$

For the diagonal matrix D, we would like it to also produce the eigenvalues after being multiplied by P. How can we do that? Let's try by putting the eigenvalues into the main diagonal of D.

$$D = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}$$

Then

$$DP = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \begin{bmatrix} v_{1,1} & v_{1,2} & v_{1,3} \\ v_{2,1} & v_{2,2} & v_{2,3} \\ v_{3,1} & v_{3,2} & v_{3,3} \end{bmatrix} = \begin{bmatrix} \lambda_1 \, v_{1,1} & \lambda_1 \, v_{1,2} & \lambda_1 \, v_{1,3} \\ \lambda_2 \, v_{2,1} & \lambda_2 \, v_{2,2} & \lambda_2 \, v_{2,3} \\ \lambda_3 \, v_{3,1} & \lambda_3 \, v_{3,2} & \lambda_3 \, v_{3,3} \end{bmatrix}$$
$$= PA$$

It works. So we can create P by simply stacking the eigenvectors together. We can also create D by putting the eigenvalues into the main diagonal.

Let's choose a magnitude for $\mathbf{v}_2$ and $\mathbf{v}_3$ that is easier for calculation. Choose

$$\mathbf{v}_2 = \begin{bmatrix} \frac{\mathbf{i}\sqrt{39}-1}{10} & \frac{-\mathbf{i}\sqrt{39}-9}{10} & 1 \end{bmatrix}$$

$$\mathbf{v}_3 = \begin{bmatrix} \frac{-\mathbf{i}\sqrt{39}-1}{10} & \frac{\mathbf{i}\sqrt{39}-9}{10} & 1 \end{bmatrix}$$

Then

$$P = \begin{bmatrix} \frac{25}{71} & \frac{15}{71} & \frac{31}{71} \\ \frac{\mathbf{i}\sqrt{39}-1}{10} & \frac{-\mathbf{i}\sqrt{39}-9}{10} & 1 \\ \frac{-\mathbf{i}\sqrt{39}-1}{10} & \frac{\mathbf{i}\sqrt{39}-9}{10} & 1 \end{bmatrix} \qquad \text{and} \qquad D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{-\mathbf{i}\sqrt{39}-3}{20} & 0 \\ 0 & 0 & \frac{\mathbf{i}\sqrt{39}-3}{20} \end{bmatrix}$$

Using the computer to find the inverse of P:

$$P^{-1} = \begin{bmatrix} 1 & \frac{-11\mathbf{i}\sqrt{39}-31}{142} & \frac{11\mathbf{i}\sqrt{39}-31}{142} \\ 1 & \frac{281\mathbf{i}\sqrt{39}-1209}{5538} & \frac{-281\mathbf{i}\sqrt{39}-1209}{5538} \\ 1 & \frac{35\mathbf{i}\sqrt{39}+260}{923} & \frac{-35\mathbf{i}\sqrt{39}+260}{923} \end{bmatrix}$$

Then

$$A^t = P^{-1} D^n P$$
$$= \begin{bmatrix} 1 & \frac{-11\mathbf{i}\sqrt{39}-31}{142} & \frac{11\mathbf{i}\sqrt{39}-31}{142} \\ 1 & \frac{281\mathbf{i}\sqrt{39}-1209}{5538} & \frac{-281\mathbf{i}\sqrt{39}-1209}{5538} \\ 1 & \frac{35\mathbf{i}\sqrt{39}+260}{923} & \frac{-35\mathbf{i}\sqrt{39}+260}{923} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & (\frac{-\mathbf{i}\sqrt{39}-3}{20})^t & 0 \\ 0 & 0 & (\frac{\mathbf{i}\sqrt{39}-3}{20})^t \end{bmatrix} \begin{bmatrix} \frac{25}{71} & \frac{15}{71} & \frac{31}{71} \\ \frac{\mathbf{i}\sqrt{39}-1}{10} & \frac{-\mathbf{i}\sqrt{39}-9}{10} & 1 \\ \frac{-\mathbf{i}\sqrt{39}-1}{10} & \frac{\mathbf{i}\sqrt{39}-9}{10} & 1 \end{bmatrix}$$

This is the general formula obtained for A^t. It seems very messy, and somehow involves complex numbers, despite the end result not containing any. The general formula would have been cleaner and more useful if the eigenvalues are all real.

Denote a diagonal matrix $\begin{bmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{bmatrix}$ by $\quad \mathrm{diag}(a_1, a_2, \dots, a_n)$.

We have the matrix diagonalization theorem.

Theorem 3.4. In general, if an $n \times n$ matrix M with n eigenvalues λ_1 , λ_2 , ... , λ_n corresponding to n row-eigenvectors $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_n$, the general formula of M raised to a power k is

$$M^k = \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_n \end{pmatrix}^{-1} \begin{bmatrix} \lambda_1^k & 0 & \dots & 0 \\ 0 & \lambda_2^k & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n^k \end{bmatrix} \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_n \end{pmatrix}$$

3.4.4 Finding eigenvalues and eigenvectors of a matrix

Earlier, we have formed a habit of letting a computer 'magically' figure out the eigenvalues and eigenvectors for us, but there is a way to do it ourselves. First, let's talk about the **determinant** of a matrix.

Determinant of a matrix

Determinant is a number associated with a matrix, and every matrix has a single determinant. A 3 × 3 matrix, in essence, is 3 row vectors stacked together. In 3-d space, when the tails of the row vectors are moved to the same point, these row vectors form the three defining-edges of a **parallelepiped** (3-d version of a parallelogram), and the volume of the parallelepiped is the absolute value of the determinant of this matrix.

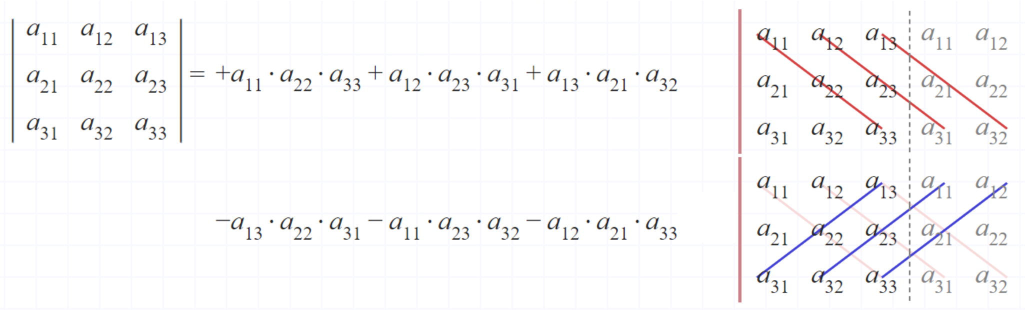
The determinant can be negative or positive, and its sign depends on the direction of the vectors. A 3 × 3 matrix with 0 as its determinant has all of its row vectors lying on the same plane.

The determinant of matrix M is denoted $|M|$ or $\det(M)$.

For example, if $M = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$, then its determinant is

$$\begin{aligned} \det(M) &= \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} \\ &= (1)(5)(9) + (2)(6)(7) + (3)(4)(8) - (3)(5)(7) - (2)(4)(9) - (1)(6)(8) \\ &= 0 \end{aligned}$$

It follows the rule of this diagram.


$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = +a_{11}\cdot a_{22}\cdot a_{33} + a_{12}\cdot a_{23}\cdot a_{31} + a_{13}\cdot a_{21}\cdot a_{32}$
$-a_{13}\cdot a_{22}\cdot a_{31} - a_{11}\cdot a_{23}\cdot a_{32} - a_{12}\cdot a_{21}\cdot a_{33}$
a_{11} a_{12} a_{13} a_{11} a_{12}
a_{21} a_{22} a_{23} a_{21} a_{22}
a_{31} a_{32} a_{33} a_{31} a_{32}
a_{11} a_{12} a_{13} a_{11} a_{12}
a_{21} a_{22} a_{23} a_{21} a_{22}
a_{31} a_{32} a_{33} a_{31} a_{32}

We can see that we add the product of entries along the red diagonal, and subtract the product of entries along the blue diagonal.

For a 2 × 2 matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $\quad \det(M) = ad - bc$

It is much simpler to calculate.

Characteristic polynomial

Recall the formula for eigenvectors:

$$\vec{v}A = \lambda\vec{v}$$

If we move the terms to one side and factor out the $\vec{v}$:

$$\begin{gathered} \vec{v}A - \lambda\vec{v} = \vec{0} \\ \vec{v}(A - \lambda I) = \vec{0} \end{gathered}$$

Let $\vec{v} = [v_1, v_2, v_3]$ and $A - \lambda I = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}$. Then

$$\vec{v}(A - \lambda I) = \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$$

Look at the three entries of RHS, which are all 0 . To get the 0 s, we are supposed to do the matrix multiplication

$$v_1\, a_{1,1} + v_2\, a_{2,1} + v_3\, a_{3,1} = 0$$

$$v_1\, a_{1,2} + v_2\, a_{2,2} + v_3\, a_{3,2} = 0$$

$$v_1\, a_{1,3} + v_2\, a_{2,3} + v_3\, a_{3,3} = 0$$

If we regard the matrix $A - \lambda I$ as three row vectors stacked together, we have

$$v_1\, \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \end{bmatrix} + v_2\, \begin{bmatrix} a_{2,1} & a_{2,2} & a_{2,3} \end{bmatrix} + v_3\, \begin{bmatrix} a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} = \vec{0}$$

Since v_1, v_2, v_3 are all non-zero scalars, by the definition of linear dependence (7), the three row vectors are linearly dependent (/not linearly independent). The geometric meaning of this is that the three row vectors lie on the same plane, so the parallelepiped spanned out by the three row vectors has a volume of 0, which in turn, means that the determinant of the matrix made up by the three row vectors is 0.

Therefore, we conclude that

$$\det(A - \lambda I) = 0$$

Substituting our transition matrix as A, we have

$$\det\left(\begin{bmatrix} 0.2 & 0.6 & 0.2 \\ 0.3 & 0 & 0.7 \\ 0.5 & 0 & 0.5 \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = 0$$

$$\begin{vmatrix} 0.2 - \lambda & 0.6 & 0.2 \\ 0.3 & 0 - \lambda & 0.7 \\ 0.5 & 0 & 0.5 - \lambda \end{vmatrix} = 0$$

$$\begin{aligned} (0.2 - \lambda)(-\lambda)(0.5 - \lambda) + (0.6)(0.7)(0.5) + (0.2)(0.3)(0) \\ -(0.2)(-\lambda)(0.5) - (0.6)(0.3)(0.5 - \lambda) - (0.2 - \lambda)(0.7)(0) &= 0 \\ -\lambda(0.1 - 0.7\lambda + \lambda^2) + 0.21 + 0.1\lambda - 0.09 + 0.18\lambda &= 0 \\ -0.1\lambda + 0.7\lambda^2 - \lambda^3 + 0.28\lambda + 0.12 &= 0 \\ \lambda^3 - 0.7\lambda^2 - 0.18\lambda - 0.12 &= 0 \end{aligned}$$

The polynomial $\lambda^3 - 0.7\lambda^2 - 0.18\lambda - 0.12$ is called the **characteristic polynomial** of the matrix A. If we solve for λ by setting the polynomial to 0, we have

$$\lambda^3 - 0.7\lambda^2 - 0.18\lambda - 0.12 = 0$$
$$(\lambda - 1)(\lambda^2 + 0.3\lambda + 0.12) = 0$$

$$\lambda = 1 \quad \textbf{or} \quad \lambda = \frac{-0.3 \pm \sqrt{0.3^2 - 4(0.12)}}{2}$$
$$= \frac{-3 \pm \sqrt{-39}}{20}$$

$$\lambda_1 = 1 \ , \ \lambda_2 = \frac{-\mathbf{i}\sqrt{39} - 3}{20} \ , \ \lambda_3 = \frac{\mathbf{i}\sqrt{39} - 3}{20}$$

We get the three eigenvalues as desired.

Theorem 3.5. The eigenvalues λ of the matrix M is given by solving the equation

$$\det(M - \lambda I) = 0$$

,which means if $M = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{bmatrix}$, then

$$\begin{vmatrix} a_{1,1} - \lambda & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} - \lambda & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} - \lambda \end{vmatrix} = 0$$

To solve for eigenvectors, just plug the values of λ into the equation $\vec{v}(A - \lambda I) = \vec{0}$, and solve for the homogeneous system of linear equations (where all of the RHS of the equations is 0) to obtain the entries for $\vec{v}$. This system of equations has infinite solutions, so the eigenvectors can take on any magnitudes. (The steps required to solve for the eigenvectors is left as an exercise for the readers.)

3.4.5 Inverse of a matrix

Finding the inverse of a 3×3 matrix M is a complicated procedure. A matrix has an inverse if and only if its determinant is not zero. We call the matrix that has an inverse a **non-singular/ invertible** matrix. In short, if $M = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}$ is a non-singular matrix, then its inverse is:

$$M^{-1} = \frac{1}{\det(M)} \begin{bmatrix} \begin{vmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} & -\begin{vmatrix} a_{2,1} & a_{2,3} \\ a_{3,1} & a_{3,3} \end{vmatrix} & \begin{vmatrix} a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} \end{vmatrix} \\ -\begin{vmatrix} a_{1,2} & a_{1,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} & \begin{vmatrix} a_{1,1} & a_{1,3} \\ a_{3,1} & a_{3,3} \end{vmatrix} & -\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{3,1} & a_{3,2} \end{vmatrix} \\ \begin{vmatrix} a_{1,2} & a_{1,3} \\ a_{2,2} & a_{2,3} \end{vmatrix} & -\begin{vmatrix} a_{1,1} & a_{1,3} \\ a_{2,1} & a_{2,3} \end{vmatrix} & \begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} \end{bmatrix}^T$$

where T denotes the **transpose** of the matrix. Taking the transpose of the matrix is just flipping the matrix with the diagonal as the axis. So

$$M^{-1} = \frac{1}{\det(M)} \begin{bmatrix} \begin{vmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} & -\begin{vmatrix} a_{1,2} & a_{1,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} & \begin{vmatrix} a_{1,2} & a_{1,3} \\ a_{2,2} & a_{2,3} \end{vmatrix} \\ -\begin{vmatrix} a_{2,1} & a_{2,3} \\ a_{3,1} & a_{3,3} \end{vmatrix} & \begin{vmatrix} a_{1,1} & a_{1,3} \\ a_{3,1} & a_{3,3} \end{vmatrix} & -\begin{vmatrix} a_{1,1} & a_{1,3} \\ a_{2,1} & a_{2,3} \end{vmatrix} \\ \begin{vmatrix} a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} \end{vmatrix} & -\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{3,1} & a_{3,2} \end{vmatrix} & \begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} \end{bmatrix}$$

The derivation of this formula is left as an exercise for the readers.

3.4.6 Finding t-step transition probability using matrix diagonalization

Problem 72. Demetrius goes to a restaurant every day, and will have either meal A, meal B, or meal C that day. The probability of the meal he chooses that day depends on the meal he chose the previous day, given by the table below:

Today Yesterday	Meal A	Meal B	Meal C
Meal A	0.5	0.3	0.2
Meal B	0.4	0.1	0.5
Meal C	0.6	0.3	0.1

If Demetrius has meal C in a particular day, what is the probability that he will have meal B 30 days later? (Express the answer as a **reduced fraction**.)

(Difficulty level: 8)

Solution 72. Let the transition matrix $A = \begin{bmatrix} 0.5 & 0.3 & 0.2 \\ 0.4 & 0.1 & 0.5 \\ 0.6 & 0.3 & 0.1 \end{bmatrix}$

The eigenvalues of A can be found by:

$$\begin{vmatrix} 0.5-\lambda & 0.3 & 0.2 \\ 0.4 & 0.1-\lambda & 0.5 \\ 0.6 & 0.3 & 0.1-\lambda \end{vmatrix} = 0$$

$$(0.5-\lambda)(0.1-\lambda)(0.1-\lambda) + (0.3)(0.5)(0.6) + (0.2)(0.4)(0.3)$$
$$-(0.2)(0.1-\lambda)(0.6) - (0.3)(0.4)(0.1-\lambda)) - (0.5-\lambda)(0.5)(0.3) = 0$$
$$-\lambda^3 + 0.7\lambda^2 + 0.28\lambda + 0.02 = 0$$
$$\lambda_1 = 1 \qquad \lambda_2 = -0.1 \qquad \lambda_3 = -0.2$$

For $\lambda_1 = 1$, we can find the row-eigenvector by substituting λ_1 into $(A - \lambda I) = 0$ and taking the transpose of A to be the augmented matrix. Then we solve by **Gaussian elimination**.

$$\left[\begin{array}{ccc|c} 0.5-1 & 0.4 & 0.6 & 0 \\ 0.3 & 0.1-1 & 0.3 & 0 \\ 0.2 & 0.5 & 0.1-1 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} -5 & 4 & 6 & 0 \\ 3 & -9 & 3 & 0 \\ 2 & 5 & -9 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|c} -5 & 4 & 6 & 0 \\ 0 & -33 & 33 & 0 \\ 0 & -33 & 33 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|c} -5 & 4 & 6 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

$$z = t, \quad y = t, \quad x = 2t \quad \Rightarrow \mathbf{v}_1 = \begin{bmatrix} 2 & 1 & 1 \end{bmatrix}$$

Similarly, for $\lambda_2 = -0.1$,

$$\left[\begin{array}{ccc|c} 0.5-(-0.1) & 0.4 & 0.6 & 0 \\ 0.3 & 0.1-(-0.1) & 0.3 & 0 \\ 0.2 & 0.5 & 0.1-(-0.1) & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 6 & 4 & 6 & 0 \\ 3 & 2 & 3 & 0 \\ 2 & 5 & 2 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|c} 3 & 2 & 3 & 0 \\ 0 & -11 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

$$z = t, \quad y = 0, \quad x = -t \quad \Rightarrow \mathbf{v}_2 = \begin{bmatrix} -1 & 0 & 1 \end{bmatrix}$$

For $\lambda_3 = -0.2$,

$$\left[\begin{array}{ccc|c} 0.5 - (-0.2) & 0.4 & 0.6 & 0 \\ 0.3 & 0.1 - (-0.2) & 0.3 & 0 \\ 0.2 & 0.5 & 0.1 - (-0.2) & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 7 & 4 & 6 & 0 \\ 3 & 3 & 3 & 0 \\ 2 & 5 & 3 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|c} 1 & 1 & 1 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

$$z = t, \quad y = -\frac{1}{3}t, \quad x = -\frac{2}{3}t \quad \Rightarrow \mathbf{v}_3 = \begin{bmatrix} -2 & -1 & 3 \end{bmatrix}$$

Stack the eigenvectors together to make a matrix P.

$$P = \begin{bmatrix} 2 & 1 & 1 \\ -1 & 0 & 1 \\ -2 & -1 & 3 \end{bmatrix}$$

$$P^{-1} = \frac{1}{\det(P)} \begin{bmatrix} \begin{vmatrix} 0 & 1 \\ -1 & 3 \end{vmatrix} & -\begin{vmatrix} -1 & 1 \\ -2 & 3 \end{vmatrix} & \begin{vmatrix} -1 & 0 \\ -2 & -1 \end{vmatrix} \\ -\begin{vmatrix} 1 & 1 \\ -1 & 3 \end{vmatrix} & \begin{vmatrix} 2 & 1 \\ -2 & 3 \end{vmatrix} & -\begin{vmatrix} 2 & 1 \\ -2 & -1 \end{vmatrix} \\ \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} & -\begin{vmatrix} 2 & 1 \\ -1 & 1 \end{vmatrix} & \begin{vmatrix} 2 & 1 \\ -1 & 0 \end{vmatrix} \end{bmatrix}^T$$

$$P^{-1} = \frac{1}{4} \begin{bmatrix} 1 & -4 & 1 \\ 1 & 8 & -3 \\ 1 & 0 & 1 \end{bmatrix}$$

$$
\begin{aligned}
A^{30} &= P^{-1}DP \\
&= \frac{1}{4}\begin{bmatrix} 1 & -4 & 1 \\ 1 & 8 & -3 \\ 1 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1^{30} & 0 & 0 \\ 0 & (-0.1)^{30} & 0 \\ 0 & 0 & (-0.2)^{30} \end{bmatrix}\begin{bmatrix} 2 & 1 & 1 \\ -1 & 0 & 1 \\ -2 & -1 & 3 \end{bmatrix} \\
&= \frac{1}{4}\begin{bmatrix} 1 & -4(0.1)^{30} & (0.2)^{30} \\ 1 & 8(0.1)^{30} & -3(0.2)^{30} \\ 1 & 0 & 0.2^{30} \end{bmatrix}\begin{bmatrix} 2 & 1 & 1 \\ -1 & 0 & 1 \\ -2 & -1 & 3 \end{bmatrix} \\
&= \frac{1}{4}\begin{bmatrix} 2+4(0.1)^{30}-2(0.2)^{30} & 1-(0.2)^{30} & 1-4(0.1)^{30}+3(0.2)^{30} \\ 2-8(0.1)^{30}+6(0.2)^{30} & 1+3(0.2)^{30} & 1+8(0.1)^{30}-9(0.2)^{30} \\ 2-2(0.2)^{30} & 1-(0.2)^{30} & 1+3(0.2)^{30} \end{bmatrix}
\end{aligned}
$$

Note that when the initial state vector $[0,0,1]$ is multiplied by A^{30} , only the bottom row of A^{30} will be recorded in $\vec{v_{30}}$. So

$$
\begin{aligned}
\vec{v_{30}} &= \begin{bmatrix} \dfrac{2-2(0.2)^{30}}{4} & \dfrac{1-(0.2)^{30}}{4} & \dfrac{1+3(0.2)^{30}}{4} \end{bmatrix} \\
&= \begin{bmatrix} \dfrac{2(10)^{30}-2^{31}}{4(10)^{30}} & \dfrac{10^{30}-2^{30}}{4(10)^{30}} & \dfrac{10^{30}+3(2)^{30}}{4(10)^{30}} \end{bmatrix}
\end{aligned}
$$

The 2nd entry corresponds to the probability of having meal B in day 30. So

$P(\text{meal B 30 days later})$

$$
= \frac{10^{30}-2^{30}}{4(10)^{30}}
$$

$$
= \frac{249999999999999999999731564544}{1000000000000000000000000000000} = \boxed{\frac{232\,830\,643\,653\,869\,628\,906}{931\,322\,574\,615\,478\,515\,625}}
$$

3.4.7 How t-step transition matrix encodes probabilities

From the problem, we see that the matrix A^{30} has already encoded the probability distribution of choosing meals in day 30. The 1st row corresponds to the probability distribution when starting with meal A in day 0, and 2nd row with meal B, and 3rd row with meal C. So in the problem, we could have saved some time by only multiplying the bottom rows of the matrices.

In general, we have the theorem:

Theorem 3.6. When there are N states labelled '1', '2', ..., 'N' in a Markov chain, (with the transition matrix A encoding the probabilities in ascending order of the states), and initially (step=0) the pointer is at state i, then the probability of reaching state j at step t is the entry in the i th row and j th column of matrix A^t.
Mathematically, for the t-step transition probability, we have

$$P(X_t = j \,|\, X_0 = i) = (A^t)_{i\,j}$$

where X_t is the random variable (location of the pointer) at step t, and $(A^t)_{i\,j}$ denotes the entry in the i th row and j th column of matrix A^t .

Note: $P(X_t = j \,|\, X_0 = i)$ can also be written as $P_{ij}^{(t)}$ or $P_i(X_t = j)$.

Explanation of how to get the equation [47]

The equation in the theorem follows from the **Chapman-Kolmogorov equation**, which states that

$$P_{ij}^{(t)} = \sum_{k=1}^{N} P_{ik}^{(r)} P_{kj}^{(t-r)} \qquad \text{, for any } r = 0, 1, 2, \ldots, t \tag{1}$$

and here's the proof:

Proof.

$$\begin{aligned}
P_{ij}^{(t)} &= P_i(X_t = j) \\
&= \sum_{k=1}^{N} P_i(X_t = j \,|\, X_r = k) P_i(X_r = k) && \text{(Law of total probability)} \\
&= \sum_{k=1}^{N} P(X_t = j \,|\, X_r = k, X_0 = i) P(X_r = k \,|\, X_0 = i) \\
&= \sum_{k=1}^{N} P(X_t = j \,|\, X_r = k) P(X_r = k \,|\, X_0 = i) && \text{(Markov property)} \\
&= \sum_{k=1}^{N} P_{ik}^{(r)} P_{kj}^{(t-r)}
\end{aligned}$$

□

If we encode the t-step transition probability from state i to state j (for all i, $j \in \{1, \ldots, N\}$) in a transition matrix $A^{(t)}$ (which is not shown to be

$= A^t$ yet) , we have:

$$(A^{(t)})_{ij} = P_{ij}^{(t)}$$

Using Chapman-Kolmogorov equation, we will find that it is similar to the way that matrix multiplication works:

$$\begin{aligned} P_{ij}^{(t)} &= \sum_{k=1}^{N} P_{ik}^{(r)} P_{kj}^{(t-r)} \\ (A^{(t)})_{ij} &= \sum_{k=1}^{N} (A^{(r)})_{ik} (A^{(t-r)})_{kj} \\ &= (A^{(r)} A^{(t-r)})_{ij} \\ A^{(t)} &= A^{(r)} A^{(t-r)} \qquad (2) \end{aligned}$$

Let $r = 1$ and expand repeatedly:

$$A^{(t)} = AA^{(t-1)} = A(AA^{(t-2)}) = A^2 A^{(t-2)} = \ldots = A^t A^0 = A^t$$

Thus, we have shown that $A^{(t)} = A^t$ for all $t \in \mathbb{Z}^+$. So we conclude that

$$P(X_t = j \,|\, X_0 = i) = P_{ij}^{(t)} = (A^{(t)})_{ij} = (A^t)_{ij}$$

3.4.8 Visiting a state 0 or 1 times

Now, what if I want to find the probability that the pointer never reach one of the states during its journey?

Reusing the situation in Problem 58, let's say Demetrius never have meal A in 2 consecutive days, starting from day 1. So he doesn't have meal A from day 1 to day 2. Refer to the probability table. The cells of undesired probability are coloured red.

Today Yesterday	Meal A	Meal B	Meal C
Meal A	0.5	0.3	0.2
Meal B	0.4	0.1	0.5
Meal C	0.6	0.3	0.1

If he has meal B in day 0, then the probability of not having meal A for two consecutive days is

$$P(\text{not A}) = (0.1)(0.1) + (0.5)(0.3) + (0.1)(0.5) + (0.5)(0.1) = 0.26$$

Alternatively, we can make a reduced transition matrix $R = \begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.1 \end{bmatrix}$ and reduced state vector $\vec{v_0} = \begin{bmatrix} 1 & 0 \end{bmatrix}$.

$$\vec{v_0}R = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.1 \end{bmatrix}^2 = \begin{bmatrix} 0.1 & 0.5 \end{bmatrix} \begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.1 \end{bmatrix} = \begin{bmatrix} 0.16 & 0.1 \end{bmatrix}$$

This is the probability distribution of not having meal A for two consecutive days when starting with meal B (with meal A excluded.) If we sum up the entries, we get the same probability as above.

In fact, we can evaluate the power of matrix first and it will already show the probability distribution of staring with meal B or meal C.

$$R^2 = \begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.1 \end{bmatrix}^2 = \begin{bmatrix} 0.16 & 0.1 \\ 0.06 & 0.16 \end{bmatrix}$$

If he doesn't have meal A for k consecutive days, the probability distribution of starting with meal B or meal C is:

$$R^k = \begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.1 \end{bmatrix}^k$$

$$= \frac{1}{10^k} \begin{bmatrix} \dfrac{(-14)^k + (2\sqrt{15}+16)^k}{2(\sqrt{15}+1)^k} & \dfrac{-(-14)^k\sqrt{15} + (2\sqrt{15}+16)^k\sqrt{15}}{6(\sqrt{15}+1)^k} \\ \dfrac{-(-14)^k\sqrt{15} + (2\sqrt{15}+16)^k\sqrt{15}}{10(\sqrt{15}+1)^k} & \dfrac{(-14)^k + (2\sqrt{15}+16)^k}{2(\sqrt{15}+1)^k} \end{bmatrix}$$

If given that he has meal A at day 0, to find the probability of not having meal A for the next k consecutive days, we can just convert one of the R into [0.3, 0.2] and sum up the entries:

$$P(\text{this}) = \text{sum}(\vec{v_1}R^{k-1}) = \text{sum}\left(\begin{bmatrix} 0.3 & 0.2 \end{bmatrix} \begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.1 \end{bmatrix}^{k-1} \right)$$

where $\text{sum}(\vec{v})$ denotes the sum of entries of vector $\vec{v}$.

If given that he has meal B at day 0, to find the probability that he does not have meal A until day k, we can insert a column vector that contains the probabilities of B → A and C → A at the right:

$$P(\text{this}) = \vec{v_0}R^{k-1} \begin{bmatrix} (A)_{2,1} \\ (A)_{3,1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 0.1 & 0.5 \\ 0.3 & 0.1 \end{bmatrix}^{k-1} \begin{bmatrix} 0.4 \\ 0.6 \end{bmatrix}$$

(Technically, the end result is a 1×1 matrix, but we view it as equivalent to its entry if the 1×1 matrix is the final result.)

Now, what if he has meal A in exactly one of the days? Let's say he has meal A exactly once in 7 days. Then meal A can be had in day 1 or day 2 or ... or day 7. Let's say he starts with meal B in day 0, and has meal A in day 1. Then for the following 6 days, he has no meal A. The probability of all of that happening is

$$P(\text{A in day 1}) = (0.4) \text{ sum}\left(\begin{bmatrix}0.3 & 0.2\end{bmatrix}\begin{bmatrix}0.1 & 0.5\\0.3 & 0.1\end{bmatrix}^5\right) = 0.005744$$

If he still starts with meal B, and has meal A in day 2 only, then the probability is

$$P(\text{A in day 2}) = \begin{bmatrix}0.1 & 0.5\end{bmatrix}\begin{bmatrix}0.4\\0.6\end{bmatrix} \text{ sum}\left(\begin{bmatrix}0.3 & 0.2\end{bmatrix}\begin{bmatrix}0.1 & 0.5\\0.3 & 0.1\end{bmatrix}^4\right) = 0.0099416$$

If he still starts with meal B, and has meal A in day 3 only, then the probability is: (Note that $\text{sum}(\vec{v})$ can be written as $\vec{v}\begin{bmatrix}1\\1\end{bmatrix}$ for $\vec{v}$ with 2 entries.)

$$P(\text{A in day 3}) = \left(\begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}0.1 & 0.5\\0.3 & 0.1\end{bmatrix}^2\begin{bmatrix}0.4\\0.6\end{bmatrix}\right)\left(\begin{bmatrix}0.3 & 0.2\end{bmatrix}\begin{bmatrix}0.1 & 0.5\\0.3 & 0.1\end{bmatrix}^3\begin{bmatrix}1\\1\end{bmatrix}\right)$$
$$= 0.0075392$$

If he starts with meal B, and has meal A in day k only (for $k \leq 6$), then the probability is:

$$P(\text{A in day k}) = \left(\begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}0.1 & 0.5\\0.3 & 0.1\end{bmatrix}^{k-1}\begin{bmatrix}0.4\\0.6\end{bmatrix}\right)\left(\begin{bmatrix}0.3 & 0.2\end{bmatrix}\begin{bmatrix}0.1 & 0.5\\0.3 & 0.1\end{bmatrix}^{6-k}\begin{bmatrix}1\\1\end{bmatrix}\right)$$

So if he starts with meal B, then the probability that he will have exactly one meal A in the next 7 day is

$$\begin{aligned}&P(\text{A exactly once})\\&= \sum_{k=0}^{6}\left(\begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}0.1 & 0.5\\0.3 & 0.1\end{bmatrix}^{k-1}\begin{bmatrix}0.4\\0.6\end{bmatrix}\right)\left(\begin{bmatrix}0.3 & 0.2\end{bmatrix}\begin{bmatrix}0.1 & 0.5\\0.3 & 0.1\end{bmatrix}^{6-k}\begin{bmatrix}1\\1\end{bmatrix}\right)\\&+ \left(\begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}0.1 & 0.5\\0.3 & 0.1\end{bmatrix}^7\begin{bmatrix}0.4\\0.6\end{bmatrix}\right)\end{aligned}$$

For the probability of having a meal exactly twice or more in the next k days, the calculation is complicated and is outside the scope of my comprehension. So we'd better use code to solve it for us.

Problem 73. Shane goes to the saloon every day, and will have a can of beer of either brand A, brand B, or brand C that day. The probability of the brand of beer he chooses that day depends on the brand of beer he chose yesterday, given by the table below:

Today Yesterday	Brand A	Brand B	Brand C
Brand A	0.3	0.6	0.1
Brand B	0.2	0.5	0.3
Brand C	0.7	0.1	0.2

If Shane has a can of brand A beer in a particular day, what is the probability that he will have 7 or more cans of brand B beer in the next 14 days? (Express the answer as a **reduced fraction**.)

(Difficulty level: 9)

Solution 73. Use python code to count every possible outcome and sum the probabilities of all the desired outcomes (desired trajectories / sequences of visited states) of the Markov chain.

```
import math, itertools
def rep(n,k):
    return list(itertools.product(list(range(0,n)),repeat=k))

def mark(x):
    A = [[3, 6, 1], [2, 5, 3], [7, 1, 2]]
    p = 1
    for i, n in enumerate(x):
        if i==0: continue
        prev = x[i-1]
        p *= A[prev][n]
    return p

seq = [i for i in rep(3,15) if i.count(1)>=7 and i[0]==0]
s=0
for i in seq:
        s += mark(i)
print(s/10**14)
```

And we get

```
0.4822743453125
```

which means

$$P(7 \text{ or more brand B beers}) = \frac{4822743453125}{10000000000000} = \boxed{\frac{308\,655\,581}{640\,000\,000}}$$

Discussion 73. We should not be too reliant on this method because it scales badly with the number of steps of the Markov chain (time complexity of about $O(3^N)$). This method is basically a brute force method, which is inelegant.

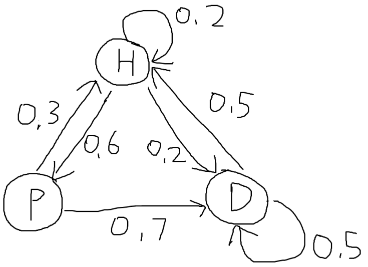
3.4.9 Markov chains with absorbing states

Irreducible Markov chains

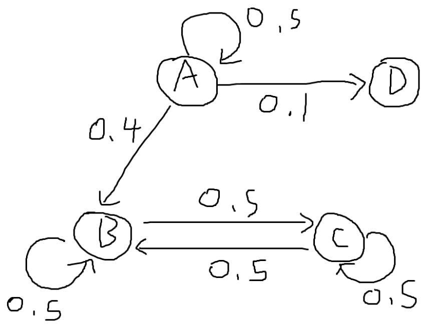
A Markov chain is said to be **irreducible** if each of the states is accessible / reachable from other states. It can take more than one steps to go from one state to another, but for any two states i and j in the Markov chain, there must be some way to go from i to j and some way to go from j to i. If that's the case, we say that i **communicates** with j, denoted by $i \leftrightarrow j$.

To be precise, let S denotes the set of all states of a Markov chain (called the **state space**). The Markov chain is irreducible if $i \leftrightarrow j$ for all $i, j \in S$.

All of the Markov chains we have talked about earlier is irreducible, such as this one:



If a Markov chain is not irreducible (/is reducible), then there exists two states i, j such that i does not communicate with j. An example of reducible Markov chain is:



We can see that state A does not communicate with state B, C and D in the Markov chain.

Recurrent states

If a Markov chain with a finite number of states is irreducible, then after infinite steps (this is a short way of saying after t steps as $t \to \infty$), every state will eventually be reached at some time with probability 1.

To see why, first let p_{ij} denote the lowest possible probability of travelling from state i to state j without visiting any state more than once, and let N_{ij} be the corresponding number of steps required to travel from i to j. If we fix a particular destination state j, there exists some starting state k such that p_{kj} is the minimum among the p_{ij} s.

If we are at state k, then after N_{kj} steps of random walking, we may or may not end up at j. Let's say we end up at some state called k_2 instead, which may or may not be k. We know that $p_{k_2j} \geq p_{kj}$.

By the **Murphy's law**, anything that has a non-zero probability to happen will eventually happen after an infinite number of (independent) trials. To explain why, let A_n denotes the event that the thing happens at least once in n trials, and let p be the probability that the thing happens in a single trial. Let's consider the complement of A_n, which is that the thing never happens after n trials. We know that for $p > 0$,

$$\lim_{n\to\infty} P((A_n)') = \lim_{n\to\infty}(1-p)^n = 0$$

since $1 - p < 1$. This means that $\lim\limits_{n\to\infty} P(A_n) = 1$.

Returning to the Markov chain, even if we assume the probability of going to state j is p_{kj} every N_k steps, there will still be a probability of 1 of eventually reaching j after infinite steps. And actually sometimes the p_{kj} is replaced by p_{k_2j}, so the actual probability is supposed to be larger or equal to that, but since probability cannot exceed 1, the actual probability of eventually going to state j is still 1.

This argument can be said for any states in the Markov chain, so eventually every state will be reached.

Moreover, by the Markov property, the pointer will 'forget' that it has reached a particular state already, so it will reach that state again, again, and again... A state that has probability 1 to be reached infinite times after infinite steps is called a **recurrent** state, So we conclude that every state is a recurrent state in an irreducible finite Markov chain.

On the other hand, a state that is not recurrent is called a **transient** state, and it will be reached only a finite number of times in infinite steps. A reducible Markov chain must have transient states, as it must have some states that are never visited again after some time.

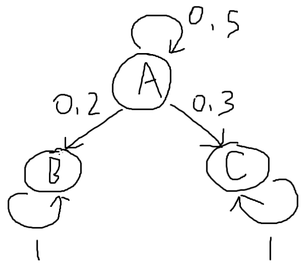
Absorbing states

(Assume that the Markov chain we're talking about has a finite number of states unless stated otherwise.)

Sometimes, we consider a random walk among the Markov chain to have ended after the pointer reaches a particular state. We can regard this state as leading to itself with probability 1. A state is called **absorbing** if the probability that it leads to itself is 1, as once the pointer has reached this absorbing state, it can never escape out of it. We can easily see that a Markov chain with absorbing states must be reducible.

If we add a single absorbing state to an otherwise irreducible Markov chain, then using the same argument above, the pointer will eventually reach the absorbing state with probability 1 and be trapped there forever.

Things get interesting when there are two absorbing states. Eventually, the pointer will reach either one of the absorbing states and be trapped there. Let's start with a simple example:



Eventually, the pointer will be trapped in B with $\frac{0.2}{0.2+0.3} = 0.4$ probability, or trapped in C with $\frac{0.3}{0.2+0.3} = 0.6$ probability.

The ratio of the hitting probabilities of the absorbing states is the same as the ratio of transition probabilities from A. However, most of the Markov chains are not as simple as this. How do we calculate the hitting probability of each absorbing state then?

Problem 74. Venus and Serena are playing tennis, and have reached the score Deuce (40-40). (Deuce comes from the French word Deux for 'two', meaning that each player needs to win two consecutive points to win the game.)

For each point, let:

$$P(\text{Venus wins point}) = 0.6, \qquad P(\text{Serena wins point}) = 0.4.$$

Assume that all points are independent. What is the probability that Venus wins the game eventually, starting from Deuce?

(Difficulty level: 7) [48]

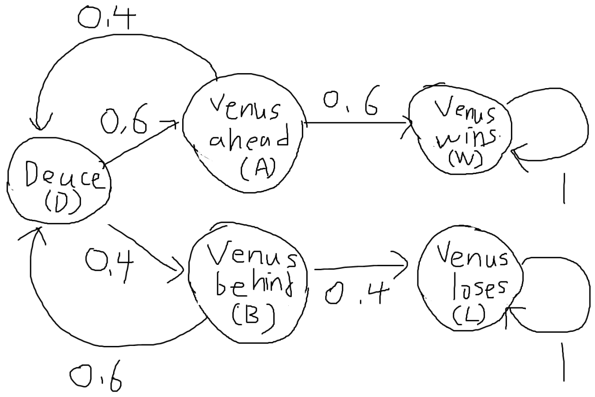
Discussion 74a. (Copied from [48]) We can use a technique called **First-Step Analysis** (FSA) to tackle this problem (this technique is also used back in Section 3.3). The idea is to consider all possible first steps away from the current state. We derive a system of equations that specify the probability of the eventual outcome given each of the possible first steps. We then try to solve these equations for the probability of interest.

First-Step Analysis depends upon conditional probability and the Partition Theorem (/Law of total probability). Let $S_1, \ldots, S_k$ be the k possible first steps we can take away from our current state. We wish to find the probability that event E happens eventually. First-Step Analysis calculates $P(E)$ as follows:

$$P(E) = P(E|S_1)P(S_1) + \ldots + P(E|S_k)P(S_k)$$

Here, $P(S_1), \ldots, P(S_k)$ give the probabilities of taking the different first steps $1, 2, \ldots, k$.

Solution 74a. We can construct a Markov chain as follows: (it looks a bit similar to a tree diagram)



Let V be the event that Venus wins eventually starting from Deuce, A be the event that Venus is ahead, B be the state that Venus is behind, D be the event that the game is at Deuce, and W be the event that Venus gets a point again when she's ahead (so she wins), L be the event that Venus does not a point again when she's behind (so she loses).

Starting from Deuce, the possible first steps are to state A and state B. We have:

$$\begin{aligned} P(V|D) &= P(V|A)P(A|D) + P(V|B)P(B|D) \\ &= 0.6P(V|A) + 0.4P(V|B) \qquad (1) \end{aligned}$$

Now We find $P(V|A)$ and $P(V|B)$, again using First-Step Analysis:

$$\begin{aligned} P(V|A) &= P(V|W)P(W|A) + P(V|D)P(D|A) \\ &= 0.6(1) + 0.4P(V|D) \qquad (2) \end{aligned}$$

Similarly,

$$\begin{aligned} P(V|B) &= P(V|L)P(L|B) + P(V|D)P(D|B) \\ &= 0.4(0) + 0.6P(V|D) \\ &= 0.6P(V|D) \qquad (3) \end{aligned}$$

Putting (2), (3) into (1):

$$\begin{aligned} P(V|D) &= 0.6(0.6 + 0.4P(V|D)) + 0.4(0.6P(V|D)) \\ &= 0.36 + 0.24P(V|D) + 0.24P(V|D) \\ P(V|D) &= \boxed{\frac{9}{13}} \end{aligned}$$

Solution 74b. We can use a transition matrix to represent the Markov chain, in the order of states (L), (B), (D), (A), (W).

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0.4 & 0 & 0.6 & 0 & 0 \\ 0 & 0.4 & 0 & 0.6 & 0 \\ 0 & 0 & 0.4 & 0 & 0.6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Notice that there are two absorbing states.

Let P_{ij} be the probability of eventually reaching state j when starting in state i, and $P_{ij}^{(t)}$ be the t-step transition probability from i to j.

Considering $X_0 = D$, we obtain

$$\begin{aligned} P_{DW} &= P_{BW}P_{DB}^{(1)} + P_{AW}P_{DA}^{(1)} \\ &= 0.4P_{BW} + 0.6P_{AW} \end{aligned} \tag{1}$$

$$\begin{aligned} P_{BW} &= P_{LW}P_{DB}^{(1)} + P_{DW}P_{BD}^{(1)} \\ &= (0)P_{DB} + 0.6P_{DW} \end{aligned} \tag{2}$$

$$\begin{aligned} P_{AW} &= P_{WW}P_{AW}^{(1)} + P_{DW}P_{AD}^{(1)} \\ &= (1)(0.6) + (0.4)P_{DW} \end{aligned} \tag{3}$$

Solving, we get $P_{DW} = \boxed{\frac{9}{13}}$

Discussion 74b. This solution is basically the same as the previous one, just using different notations (Oops, my bad for being repetitive.). But now we know that when there are two absorbing states or more, we can use First-Step Analysis to set up a system of equations to find the desired probability.

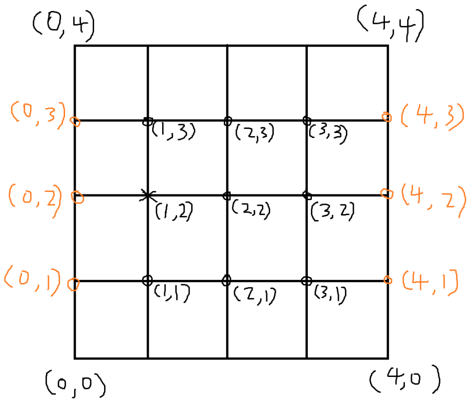
By the way, this problem is equivalent to the integer line randomly walk, with $a = 2$ and $b = 4$, so we can use the formula from Theorem 3.3 too.

Now what about a random walk in the 2D plane?

Problem 75. A frog sitting at the point $(1, 2)$ in the Cartesian plane begins a sequence of jumps, where each jump is parallel to one of the coordinate axes and has length 1, and the direction of each jump (up, down, right, or left) is chosen independently at random. The sequence ends when the frog reaches a **side** of the square with vertices $(0, 0), (0, 4), (4, 4)$, and $(4, 0)$. What is the probability that the sequence of jumps ends on a vertical side of the square?

(Difficulty level: 7) [49] (2020 AMC 10A Problems/Problem 13)

Solution 75a. We can visualize the situation with a diagram: (orange points are the desired points)



(Copied from [49] Solution 4) Let $P_{(x,y)}$ denote the probability of the frog's sequence of jumps ends with it hitting a vertical edge when it is at (x, y). Note that $P_{(1,2)} = P_{(3,2)}$ by reflective symmetry over the line $x = 2$. Similarly, $P_{(1,1)} = P_{(1,3)} = P_{(3,1)} = P_{(3,3)}$, and $P_{(2,1)} = P_{(2,3)}$. Now we create equations for the probabilities at each of these points/states by considering the probability of going either up, down, left, or right from that point:

$$P_{(1,2)} = \frac{1}{4} + \frac{1}{2}P_{(1,1)} + \frac{1}{4}P_{(2,2)}$$

$$P_{(2,2)} = \frac{1}{2}P_{(1,2)} + \frac{1}{2}P_{(2,1)}$$

$$P_{(1,1)} = \frac{1}{4} + \frac{1}{4}P_{(1,2)} + \frac{1}{4}P_{(2,1)}$$

$$P_{(2,1)} = \frac{1}{2}P_{(1,1)} + \frac{1}{4}P_{(2,2)}$$

We have a system of 4 equations in 4 variables, so we can solve for each of these probabilities. Plugging the second equation into the fourth equation gives

$$P_{(2,1)} = \frac{1}{2}P_{(1,1)} + \frac{1}{4}\left(\frac{1}{2}P_{(1,2)} + \frac{1}{2}P_{(2,1)}\right)$$

$$P_{(2,1)} = \frac{8}{7}\left(\frac{1}{2}P_{(1,1)} + \frac{1}{8}P_{(1,2)}\right) = \frac{4}{7}P_{(1,1)} + \frac{1}{7}P_{(1,2)}$$

Plugging in the third equation into this gives

$$P_{(2,1)} = \frac{4}{7}\left(\frac{1}{4} + \frac{1}{4}P_{(1,2)} + \frac{1}{4}P_{(2,1)}\right) + \frac{1}{7}P_{(1,2)}$$

$$P_{(2,1)} = \frac{7}{6}\left(\frac{1}{7} + \frac{2}{7}P_{(1,2)}\right) = \frac{1}{6} + \frac{1}{3}P_{(1,2)} \text{ (*)}$$

Next, plugging in the second and third equation into the first equation yields

$$P_{(1,2)} = \frac{1}{4} + \frac{1}{2}\left(\frac{1}{4} + \frac{1}{4}P_{(1,2)} + \frac{1}{4}P_{(2,1)}\right) + \frac{1}{4}\left(\frac{1}{2}P_{(1,2)} + \frac{1}{2}P_{(2,1)}\right)$$

$$P_{(1,2)} = \frac{3}{8} + \frac{1}{4}P_{(1,2)} + \frac{1}{4}P_{(2,1)}$$

Now plugging in (*) into this, we get

$$P_{(1,2)} = \frac{3}{8} + \frac{1}{4}P_{(1,2)} + \frac{1}{4}\left(\frac{1}{6} + \frac{1}{3}P_{(1,2)}\right)$$

$$P_{(1,2)} = \frac{3}{2} \cdot \frac{5}{12} = \boxed{\frac{5}{8}}$$

Solution 75b. If the frog is on one of the 2 diagonals, the chance of landing on vertical or horizontal each becomes $\frac{1}{2}$. Since it starts on $(1,2)$, there is a $\frac{3}{4}$ chance (up, down, or right) it will reach a diagonal on the first jump and $\frac{1}{4}$ chance (left) it will reach the vertical side. The probablity of landing on a vertical is $\frac{1}{4} + \frac{3}{4} \cdot \frac{1}{2} = \boxed{\frac{5}{8}}$

Discussion 75. Although Solution b is much shorter, Solution a can be generalized to larger grids while Solution b cannot.

Hitting probability

The **hitting probability** of a state is the probability of reaching the state at least once in infinite steps. For Markov chains with absorbing states, the pointer may get absorbed into the absorbing state before it gets the chance to visit all other states, so some states may not be visited at all. These states have a probability less than 1 to be visited.

To find the hitting probability of a particular state j, we can pretend it is an absorbing state in that particular calculation, since once the pointer is in state j, it has a probability 1 to hit j. Once the pointer hits (reaches) the state for the first time, our goal is accomplished and what happens afterwards do not matter to us, so we can consider the Markov chain process to have ended.

Problem 76. There are four pads labelled '0', '1', '2', '3'. A flea is initially on pad 1 (in second 0), and in any given second $t > 0$, it will randomly choose a pad to hop onto. The probability of the pad it chooses in second t depends on the pad the flea is on in second $t - 1$. However, pad 0 is sticky and once the flea lands on it, it can never escape. The transition probability is given below:

ts $t - 1$s	Pad 0	Pad 1	Pad 2	Pad 3
Pad 0	1	0	0	0
Pad 1	0.1	0.2	0.5	0.2
Pad 2	0.1	0.2	0.6	0.1
Pad 3	0.2	0.2	0.3	0.3

What is the probability that the flea lands on pad 2 at least once?

(Difficulty level: 7) ([50] Ex.13 Modified)

Solution 76. We can view each pad as a state in a Markov chain.

Because 0 is an absorbing state, the flea will eventually end up in state 0. What we want to know is whether or not the flea visits state 2 before that point. To do this, we will stop the process if it visits state 2 by pretending that state 2 is an absorbing state:

$$A^* = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0.1 & 0.2 & 0.5 & 0.2 \\ 0 & 0 & 1 & 0 \\ 0.2 & 0.2 & 0.3 & 0.3 \end{bmatrix}$$

Then, after infinitely long time, the flea will either be absorbed into state 0 or state 2. The desired probability that the flea visits state 2 at least once is the probability it is absorbed into state 2 in this new Markov chain A^*. We compute this using a first step analysis. (The notation is similar to what used in the previous solution.)

Considering $X_0 = 1$, we obtain

$$\begin{aligned} P_{12} &= P_{10}^{(1)} P_{02} + P_{11}^{(1)} P_{12} + P_{12}^{(1)} P_{22} + P_{13}^{(1)} P_{32} \\ &= 0 + 0.2P_{12} + 0.5(1) + 0.2P_{32} \end{aligned} \tag{1}$$

$$\begin{aligned} P_{32} &= P_{30}^{(1)} P_{02} + P_{31}^{(1)} P_{12} + P_{32}^{(1)} P_{22} + P_{33}^{(1)} P_{32} \\ &= 0 + 0.2P_{12} + 0.3(1) + 0.3P_{32} \end{aligned} \tag{2}$$

Solving, $P_{12} = \frac{41}{52}$, $P_{32} = \frac{17}{26}$.

The desired probability is $P_{12} = \boxed{\dfrac{41}{52}}$.

Discussion 76. If we want to find the probability that the flea never visits state 2, we can still pretend that state 2 is an absorbing state, but now our goal is for the flea to go to state 0, and we find the probability P_{10} instead.

Reaching absorbing states in exactly t-steps

How do we find the probability of reaching an absorbing state in exactly t-steps? We can first find the probability of never reaching the absorbing state in the first $t-1$ steps and multiply it with the probability of reaching the absorbing state in the t th step. We can calculate this by excluding the absorbing state in the transition matrix (see Section 3.4.8).

Let's reuse the previous problem.

Problem 76.2. (Restated) There are four pads labelled '0', '1', '2', '3'. A flea is initially on pad 1 (in second 0), and in any given second $t > 0$, it will randomly choose a pad to hop onto. The probability of the pad it chooses in second t depends on the pad the flea is on in second $t-1$. However, pad 0 is sticky and once the flea lands on it, it can never escape. The transition probability is given below:

ts $t-1$s	Pad 0	Pad 1	Pad 2	Pad 3
Pad 0	1	0	0	0
Pad 1	0.1	0.2	0.5	0.2
Pad 2	0.1	0.2	0.6	0.1
Pad 3	0.2	0.2	0.3	0.3

What is the probability that the flea does not land on pad 0 until second 6 (/lands on pad 0 in exactly second 6 but not before)?

(Difficulty level: 7)

Solution 76.2. We can find the probability that the flea never lands on pad 0 in the first 5 seconds given that it starts on pad 1, and multiply the probability column vector $\vec{p}$ of landing on pad 0 in second 6. Let's make a reduced transition matrix.

$$R = \begin{bmatrix} 0.2 & 0.5 & 0.2 \\ 0.2 & 0.6 & 0.1 \\ 0.2 & 0.3 & 0.3 \end{bmatrix}$$

Using a computer to find the product:

$$\vec{v_0} R^5 \vec{p} = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0.2 & 0.5 & 0.2 \\ 0.2 & 0.6 & 0.1 \\ 0.2 & 0.3 & 0.3 \end{bmatrix}^5 \begin{bmatrix} 0.1 \\ 0.1 \\ 0.2 \end{bmatrix}$$

$$= \boxed{\frac{6387}{100000}}$$

3.4.10 Other applications of Markov chains

Here is another problem that we can use Markov chain to solve, even though it is not obvious.
Dice sum divisibility

Problem 77. A dice is thrown 2022 times. What is the probability that the sum of the numbers obtained is divisible by 4?

(Difficulty level: 8) [16]

Solution 77. We can do the sum in modular arithmetic, and view each remainder modulo 4 as a state. Initially, the sum is in $0 \pmod 4$, and after a dice throw, the sum can be $1, 2, 3, 0, 1, 2 \pmod 4$. There is $\frac{1}{6}$

probability each that the sum will change from 0 to 0 (mod 4) and 0 to 3 (mod 4). There is $\frac{2}{6}$ probability each that the sum will change from 0 to 1 (mod 4) and 0 to 2 (mod 4). If after some number of throws, the sum is 1 (mod 4), then the probabilities of the remainder of the sum after the next throw can just be 'shifted to the right'. Note that the probabilities of dice sum mod 4 in the $t+1$ th throw only depends on the dice sum mod 4 in the t th throw.

The transition matrix of dice sum mod 4 is (in the order 0, 1, 2, 3):

$$A = \begin{bmatrix} \frac{1}{6} & \frac{2}{6} & \frac{2}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{2}{6} & \frac{2}{6} \\ \frac{2}{6} & \frac{1}{6} & \frac{1}{6} & \frac{2}{6} \\ \frac{2}{6} & \frac{2}{6} & \frac{1}{6} & \frac{1}{6} \end{bmatrix}$$

Since we are looking for the sum from 0 to 0 (mod 4) after 2022 throws, we can look for the element in the top left corner of the matrix A^{2022}.

First we find the eigenvalues of the matrix. The determinant of a 4×4 matrix is more complicated than a 3×3 matrix and can be solved as follows:

$$\frac{1}{6^4}\begin{vmatrix} 1-6\lambda & 2 & 2 & 1 \\ 1 & 1-6\lambda & 2 & 2 \\ 2 & 1 & 1-6\lambda & 2 \\ 2 & 2 & 1 & 1-6\lambda \end{vmatrix} = 0$$

$$(1-6\lambda)\begin{vmatrix} 1-6\lambda & 2 & 2 \\ 1 & 1-6\lambda & 2 \\ 2 & 1 & 1-6\lambda \end{vmatrix} - 2\begin{vmatrix} 1 & 2 & 2 \\ 2 & 1-6\lambda & 2 \\ 2 & 1 & 1-6\lambda \end{vmatrix}$$

$$+2\begin{vmatrix} 1 & 1-6\lambda & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1-6\lambda \end{vmatrix} - (1)\begin{vmatrix} 1 & 1-6\lambda & 2 \\ 2 & 1 & 1-6\lambda \\ 2 & 2 & 1 \end{vmatrix} = 0$$

$$\begin{aligned} (1-6\lambda)((1-6\lambda)^3+8+2-4(1-6\lambda)-2(1-6\lambda)-2(1-6\lambda)) \\ -2((1-6\lambda)^2+8+4-4(1-6\lambda)-4(1-6\lambda)-2) \\ +2((1-6\lambda)+4(1-6\lambda)+8-4-4-2(1-6\lambda)^2) \\ -(1+2(1-6\lambda)^2+8-4-2(1-6\lambda)-2(1-6\lambda)) = 0 \end{aligned}$$

$$\begin{aligned}(1-6\lambda)^4 - 8(1-6\lambda)^2 + 10(1-6\lambda) - 2(1-6\lambda)^2 + 16(1-6\lambda) - 20 \\ -4(1-6\lambda)^2 + 10(1-6\lambda) - 2(1-6\lambda)^2 + 4(1-6\lambda) - 5 = 0\end{aligned}$$

Let $u = 1 - 6\lambda$.

$$\begin{aligned}u^4 - 8u^2 + 10u - 2u^2 + 16u - 20 - 4u^2 + 10u - 2u^2 + 4u - 5 = 0 \\ u^4 - 16u^2 + 40u - 25 = 0\end{aligned}$$

$$u_1 = 1 \qquad u_2 = -5 \qquad u_3 = 2 + \mathbf{i} \qquad u_4 = 2 - \mathbf{i}$$

$$\lambda_1 = 0 \qquad \lambda_2 = 1 \qquad \lambda_3 = \frac{-\mathbf{i} - 1}{6} \qquad \lambda_4 = \frac{\mathbf{i} - 1}{6}$$

Now find the eigenvectors (this time I use column eigenvectors so no need to transpose the transition matrix).

For $\lambda_1 = 0$:

$$\left[\begin{array}{cccc|c} 1 & 2 & 2 & 1 & 0 \\ 1 & 1 & 2 & 2 & 0 \\ 2 & 1 & 1 & 2 & 0 \\ 2 & 2 & 1 & 1 & 0 \end{array}\right] \sim \left[\begin{array}{cccc|c} 1 & 2 & 2 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 1 & 0 & -1 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{cccc|c} 1 & 2 & 2 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 3 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

$$x_4 = t, \;\; x_3 = -t, \;\; x_2 = t, \;\; x_1 = -t \quad \Rightarrow \quad v_1 = \begin{bmatrix} -1 \\ 1 \\ -1 \\ 1 \end{bmatrix}$$

For $\lambda_2 = 1$:

$$\left[\begin{array}{cccc|c} 1-6(1) & 2 & 2 & 1 & 0 \\ 1 & 1-6(1) & 2 & 2 & 0 \\ 2 & 1 & 1-6(1) & 2 & 0 \\ 2 & 2 & 1 & 1-6(1) & 0 \end{array}\right] \sim \left[\begin{array}{cccc|c} -5 & 2 & 2 & 1 & 0 \\ 1 & -5 & 2 & 2 & 0 \\ 2 & 1 & -5 & 2 & 0 \\ 2 & 2 & 1 & -5 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{cccc|c} -5 & 2 & 2 & 1 & 0 \\ 0 & 23 & -12 & -11 & 0 \\ 0 & -11 & 9 & 2 & 0 \\ 0 & 1 & 6 & -7 & 0 \end{array}\right] \sim \left[\begin{array}{cccc|c} -5 & 2 & 2 & 1 & 0 \\ 0 & 253 & -132 & -121 & 0 \\ 0 & 0 & -75 & 75 & 0 \\ 0 & 0 & -75 & 75 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{cccc|c} -5 & 2 & 2 & 1 & 0 \\ 0 & 253 & 0 & -253 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

$$x_4 = t, \quad x_3 = t, \quad x_2 = t, \quad x_1 = t \quad \Rightarrow \quad v_2 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

For $\lambda_3 = \dfrac{-\mathbf{i} - 1}{6}$:

$$\left[\begin{array}{cccc|c} 1-(-\mathbf{i}-1) & 2 & 2 & 1 & 0 \\ 1 & 1-(-\mathbf{i}-1) & 2 & 2 & 0 \\ 2 & 1 & 1-(-\mathbf{i}-1) & 2 & 0 \\ 2 & 2 & 1 & 1-(-\mathbf{i}-1) & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{cccc|c} 2+\mathbf{i} & 2 & 2 & 1 & 0 \\ 1 & 2+\mathbf{i} & 2 & 2 & 0 \\ 2 & 1 & 2+\mathbf{i} & 2 & 0 \\ 2 & 2 & 1 & 2+\mathbf{i} & 0 \end{array}\right] \sim \left[\begin{array}{cccc|c} 1 & 2+\mathbf{i} & 2 & 2 & 0 \\ 0 & 1+4\mathbf{i} & 2+2\mathbf{i} & 3+2\mathbf{i} & 0 \\ 0 & 3+2\mathbf{i} & 2-\mathbf{i} & 2 & 0 \\ 0 & 1 & -1-\mathbf{i} & \mathbf{i} & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{cccc|c} 1 & 2+\mathbf{i} & 2 & 2 & 0 \\ 0 & 1+4\mathbf{i} & 2+2\mathbf{i} & 3+2\mathbf{i} & 0 \\ 0 & 0 & -4+3\mathbf{i} & 3+4\mathbf{i} & 0 \\ 0 & 0 & -3-4\mathbf{i} & -4+3\mathbf{i} & 0 \end{array}\right] \sim \left[\begin{array}{cccc|c} 1 & 2+\mathbf{i} & 2 & 2 & 0 \\ 0 & 1+4\mathbf{i} & 2+2\mathbf{i} & 3+2\mathbf{i} & 0 \\ 0 & 0 & -4+3\mathbf{i} & 3+4\mathbf{i} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

$$x_4 = t, \quad x_3 = -t\,\mathbf{i}, \quad x_2 = -t, \quad x_1 = t\,\mathbf{i} \quad \Rightarrow \quad v_3 = \begin{bmatrix} -\mathbf{i} \\ -1 \\ \mathbf{i} \\ 1 \end{bmatrix}$$

Similarly for $\lambda_4 = \dfrac{\mathbf{i} - 1}{6}$:

$$x_4 = t, \quad x_3 = t\,\mathbf{i}, \quad x_2 = -t, \quad x_1 = -t\,\mathbf{i} \quad \Rightarrow \quad v_4 = \begin{bmatrix} \mathbf{i} \\ -1 \\ -\mathbf{i} \\ 1 \end{bmatrix}$$

When using column vector, we can put the eigenvectors together side by side to make P .

$$P = \begin{bmatrix} -1 & 1 & -\mathbf{i} & \mathbf{i} \\ 1 & 1 & -1 & -1 \\ -1 & 1 & \mathbf{i} & -\mathbf{i} \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\det(P) = (-1)\begin{vmatrix}1 & -1 & -1\\ 1 & \mathbf{i} & -\mathbf{i}\\ 1 & 1 & 1\end{vmatrix} - \begin{vmatrix}1 & -1 & -1\\ -1 & \mathbf{i} & -\mathbf{i}\\ 1 & 1 & 1\end{vmatrix} + (-\mathbf{i})\begin{vmatrix}1 & 1 & -1\\ -1 & 1 & -\mathbf{i}\\ 1 & 1 & 1\end{vmatrix} - (\mathbf{i})\begin{vmatrix}1 & 1 & -1\\ -1 & 1 & \mathbf{i}\\ 1 & 1 & 1\end{vmatrix}$$

$$\begin{aligned}
&= -\,(\mathbf{i}+\mathbf{i}-1+\mathbf{i}+1+\mathbf{i}) - (\mathbf{i}+\mathbf{i}+1+\mathbf{i}-1+\mathbf{i})\\
&\quad - \mathbf{i}(1-\mathbf{i}+1+1+1+\mathbf{i}) - \mathbf{i}(1+\mathbf{i}+1+1+1-\mathbf{i})\\
&\quad = -4\mathbf{i} - 4\mathbf{i} - 4\mathbf{i} - 4\mathbf{i}\\
&\quad = -16\mathbf{i}
\end{aligned}$$

The inverse of a 4×4 matrix is similar to how we find the inverse of a 3 × 3 one.

$$\begin{aligned}
P^{-1} &= \frac{1}{16}\mathbf{i}\begin{bmatrix}4\mathbf{i} & -(4\mathbf{i}) & 4 & -(4)\\ -(4\mathbf{i}) & -4\mathbf{i} & -(-4\mathbf{i}) & 4\mathbf{i}\\ 4\mathbf{i} & -(4\mathbf{i}) & -4 & -(-4)\\ -(4\mathbf{i}) & -4\mathbf{i} & -(4\mathbf{i}) & -4\mathbf{i}\end{bmatrix}^T\\
&= \frac{1}{16}\mathbf{i}\begin{bmatrix}4\mathbf{i} & -4\mathbf{i} & 4\mathbf{i} & -4\mathbf{i}\\ -4\mathbf{i} & -4\mathbf{i} & -4\mathbf{i} & -4\mathbf{i}\\ 4 & 4\mathbf{i} & -4 & -4\mathbf{i}\\ -4 & 4\mathbf{i} & 4 & -4\mathbf{i}\end{bmatrix}\\
&= \frac{1}{4}\begin{bmatrix}-1 & 1 & -1 & 1\\ 1 & 1 & 1 & 1\\ \mathbf{i} & -1 & -\mathbf{i} & 1\\ -\mathbf{i} & -1 & \mathbf{i} & 1\end{bmatrix}
\end{aligned}$$

Also, for the diagonalized form of A, P and P^{-1} switch place when compared to using row-eigenvectors to make P.

$$\begin{aligned}
A^n &= PD^nP^{-1}\\
&= \frac{1}{4}\begin{bmatrix}-1 & 1 & -\mathbf{i} & \mathbf{i}\\ 1 & 1 & -1 & -1\\ -1 & 1 & \mathbf{i} & -\mathbf{i}\\ 1 & 1 & 1 & 1\end{bmatrix}\begin{bmatrix}0 & 0 & 0 & 0\\ 0 & 1^n & 0 & 0\\ 0 & 0 & (\frac{-1-\mathbf{i}}{6})^n & 0\\ 0 & 0 & 0 & (\frac{-1+\mathbf{i}}{6})^n\end{bmatrix}\begin{bmatrix}-1 & 1 & -1 & 1\\ 1 & 1 & 1 & 1\\ \mathbf{i} & -1 & -\mathbf{i} & 1\\ -\mathbf{i} & -1 & \mathbf{i} & 1\end{bmatrix}\\
&= \frac{1}{4}\begin{bmatrix}0 & 1 & -\mathbf{i}(\frac{-1-\mathbf{i}}{6})^n & \mathbf{i}(\frac{-1+\mathbf{i}}{6})^n\\ ? & ? & ? & ?\\ ? & ? & ? & ?\\ ? & ? & ? & ?\end{bmatrix}\begin{bmatrix}-1 & 1 & -1 & 1\\ 1 & 1 & 1 & 1\\ \mathbf{i} & -1 & -\mathbf{i} & 1\\ -\mathbf{i} & -1 & \mathbf{i} & 1\end{bmatrix}
\end{aligned}$$

$$= \frac{1}{4}\begin{bmatrix}1 + (\frac{-1-\mathbf{i}}{6})^n + (\frac{-1+\mathbf{i}}{6})^n & ? & ? & ?\\ ? & ? & ? & ?\\ ? & ? & ? & ?\\ ? & ? & ? & ?\end{bmatrix}$$

We can see that the probability of the sum divisible by 4 after n throws is

$$\frac{1}{4}(1+(\frac{-1-\mathbf{i}}{6})^n+(\frac{-1+\mathbf{i}}{6})^n)$$

. Note that we can convert $(-1-\mathbf{i})$ and $(-1+\mathbf{i})$ into polar form.

$$-1-\mathbf{i}=\sqrt{2}(\cos 225^\circ+\sin 225^\circ) \quad \text{and} \quad -1+\mathbf{i}=\sqrt{2}(\cos 135^\circ+\sin 135^\circ)$$

So by de Moivre's formula, we have

$$\begin{aligned}&(\frac{-1-\mathbf{i}}{6})^{2022}+(\frac{-1+\mathbf{i}}{6})^{2022}\\ &=\frac{\sqrt{2}^{2022}}{6^{2022}}(\cos(2022\cdot 225^\circ)+\sin(2022\cdot 225^\circ)+\cos(2022\cdot 135^\circ)+\sin(2022\cdot 135^\circ))\\ &=\frac{\sqrt{2}^{2022}}{6^{2022}}(\cos(270^\circ)+\sin(270^\circ)+\cos(90^\circ)+\sin(90^\circ))\\ &=0\end{aligned}$$

Thus, P(sum divisible by 4)= $\boxed{\frac{1}{4}}$. ('Obvious' answer)

Yahtzee probability

Problem 78. I am playing a dice game. In the first roll, I roll five dice at the same time. Then for each of the following rolls, I only re-roll all the dice that do not land on a '6'. This is repeated until all the five dice are on '6'. What is the probability I need at most 3 rolls?

(Difficulty level: 8)

Solution 78. Let's use the binomial formula to find the probability of getting k '6's in a roll. We have

$$P(k)=(\frac{1}{6^5})C_k^5(\frac{1}{6})^k(\frac{5}{6})^{5-k}$$

Evaluating $P(k)$ for each k in $\{0,1,2,3,4,5\}$:

k	0	1	2	3	4	5
$P(k)$	$\frac{3125}{7776}$	$\frac{3125}{7776}$	$\frac{1250}{7776}$	$\frac{250}{7776}$	$\frac{25}{7776}$	$\frac{1}{7776}$

From this it follows that if we have i '6's before a roll, then after the roll we will have $i+k$ '6's with probability

$$C_k^{5-i}(\frac{1}{6})^k(\frac{5}{6})^{5-(i+k)}$$

Evaluating these probabilities, we can construct a transition matrix A for the number of '6's obtained as follows:

from / to	0	1	2	3	4	5
0	$\frac{3125}{7776}$	$\frac{3125}{7776}$	$\frac{1250}{7776}$	$\frac{250}{7776}$	$\frac{25}{7776}$	$\frac{1}{7776}$
1	0	$\frac{625}{1296}$	$\frac{500}{1296}$	$\frac{150}{1296}$	$\frac{20}{1296}$	$\frac{1}{1296}$
2	0	0	$\frac{125}{216}$	$\frac{75}{216}$	$\frac{15}{216}$	$\frac{1}{216}$
3	0	0	0	$\frac{25}{36}$	$\frac{10}{36}$	$\frac{1}{36}$
4	0	0	0	0	$\frac{5}{6}$	$\frac{1}{6}$
5	0	0	0	0	0	1

Let the initial state vector $\vec{v}$ be $\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$. Compute $\vec{v}A^3$:

$$\vec{v}A^3 = \begin{bmatrix}\frac{30517578125}{470184984576} & \frac{111083984375}{470184984576} & \frac{80869140625}{235092492288} & \frac{58872734375}{235092492288} & \frac{42859350625}{470184984576} & \frac{6240321451}{470184984576}\end{bmatrix}$$

The last entry of $\vec{v}A^3$ is the desired probability, so

$$P(\text{at most 3 rolls}) = \boxed{\frac{6240321451}{470184984576}}$$

What if any number from $\{1, 2, 3, 4, 5, 6\}$ for the 5-of-a-kind of the dice (called a Yahtzee) is desired, and we play strategically?

Problem 79. I am playing a dice game called Yahtzee, in which I need to try to get five dice to be on the same number after a total of 3 rolls.

In the first roll, I roll five dice at the same time. After the first roll, I may choose some dice to keep and other dice to be re-rolled in the second roll. There are three situations that can happen:

(i) There is a unique most common number rolled: I keep the dice of the most common number rolled and then re-roll all the other dice to see if I can end up with more of that number. (If the five dice are already on the same number, then I re-roll nothing in the following rolls.)

(ii) There is a tie of several most common numbers: I randomly choose one of the most common numbers and keep only the dice with that number.

(iii) The six dice have all different numbers: I re-roll all five of the dice.

For example of (ii), if the five dice after the first roll is $[2, 2, 3, 3, 1]$, then I will randomly choose between '2' and '3' to keep the two dice with that chosen number. Then the other three dice are re-rolled in the next roll.

After the second roll, how I keep or re-roll the dice is similar to after the first roll, but if another number appear more times than the number kept in the first roll, I will change the number that I am seeking to the more favourable number. For example, if I keep two '4's after the first roll but roll three '5's in the second roll, I will keep the three '5's instead and re-roll the two '4's to try for a Yahtzee in '5's in the third roll.

What is the probability I have all five dice on the same number (getting a 'Yahtzee') after the 3 rolls? (Express the answer as a percentage cor. to 2 d.p.)

(Difficulty level: 9) [51]

Solution 79. ([51] p.8-10) There are $6^5 = 7776$ outcomes for the first roll. The number of these that lead to the different hand patterns are as follows:

Pattern	Formula for Outcomes	Total Outcomes
5	6	6
4, 1	$6 \cdot C^5_4 \cdot 5$	150
3, 2	$6 \cdot C^5_3 \cdot 5$	300
3, 1, 1	$6 \cdot C^5_3 \cdot 5 \cdot 4$	1200
2, 2, 1	$C^6_2 \cdot C^4_2 \cdot C^3_2 \cdot 4$	1800
2, 1, 1, 1	$6 \cdot C^5_2 \cdot 5 \cdot 4 \cdot 3$	3600
1, 1, 1, 1, 1	$6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$	720

To explain, ' 4, 1 ' means four of one number and one of another. There are 6 values we can pick for the four of a kind, C^5_4 ways of picking the dice that will show this number, and 5 values to assign to the remaining one dice. The hand 2, 2, 1 is perhaps the trickiest. There are C_2^6 ways of picking the two values that will appear twice, C_2^5 ways of picking the two dice that will show the higher pair, C_2^3 ways of picking the dice for the lower pair, and 4 values for the remaining one dice.

If we keep the most common number then the number of copies we have will be

Number of copies, i	1	2	3	4	5
Total outcomes	720	5400	1500	150	6
Probability, $q(i)$	$\frac{120}{1296}$	$\frac{900}{1296}$	$\frac{250}{1296}$	$\frac{25}{1296}$	$\frac{1}{1296}$

We can construct a transition matrix similar to the one in the solution of the previous problem, but the states are the number of the most common number(s) instead of number of '6's. Note that after the first roll, it is impossible for the number of the most common number to be zero, so we do not include the column and row of the '0' state.

Note that if we already have three or more of the same number, then we will not change the number we are seeking; at most we could end up with two of some other number after our next roll. Also, the transition probabilities after getting 3-of-a-kind are the same for each number in $\{1, 2, 3, 4, 5, 6\}$ because of symmetry. Therefore the bottom three rows of our transition matrix is same as that in the solution of the previous problem.

If we get all different numbers after one of our rolls, then we are going to re-roll all of the dice (it would not affect our Yahtzee probability if instead we kept one die, can you see why?). Therefore the elements of the first row of our new transition matrix are just the probabilities $q(i)$ of getting i of a kind on our first roll.

For the second row, we begin by noting that if we are keeping two dice of some number then we can not get four or five of another number on the next roll, so if the number of most common number is 4 or 5, then the most common number must be the same number as the original number. Therefore the one step transition probabilities
$P(2 \to 4) = C_2^3(\frac{1}{6})^2(\frac{5}{6}) = \frac{15}{216}$ and $P(2 \to 5) = (\frac{1}{6})^3 = \frac{1}{216}$.

For calculating $P(2 \to 3)$, there can be exactly one of the three re-rolled dice getting the original number with probability $C_1^3(\frac{1}{6})(\frac{5}{6})^2 = \frac{75}{216}$. However, it is possible that all three of the dice that we re-roll will be the same number but different from our original number. Since there are five different numbers that we could roll, this occurs with probability $5 \cdot (\frac{1}{6})^3 = \frac{5}{216} \cdot$ The two situations give a total probability of $P(2 \to 3) = \frac{80}{216}$. Since $P(2 \to 1) = 0$,

$$P(2 \to 2) = 1 - P(2 \to 5) - P(2 \to 4) - P(2 \to 3) = \frac{120}{216}$$

Therefore, our new transition matrix is:

from / to	1	2	3	4	5
1	$\frac{120}{1296}$	$\frac{900}{1296}$	$\frac{250}{1296}$	$\frac{25}{1296}$	$\frac{1}{1296}$
2	0	$\frac{120}{216}$	$\frac{80}{216}$	$\frac{15}{216}$	$\frac{1}{216}$
3	0	0	$\frac{25}{36}$	$\frac{10}{36}$	$\frac{1}{36}$
4	0	0	0	$\frac{5}{6}$	$\frac{1}{6}$
5	0	0	0	0	1

In this problem we re-rolled if we had no matching dice. Therefore, before our first roll we are in the same situation as if we had rolled no matching dice on the previous turn, which means we can pretend that we start at state 1. Therefore, taking the cube of the transition matrix, the first row will give us the probability of each outcome after three turns. The cubed transition matrix is:

from / to	1	2	3	4	5
1	$\frac{125}{157464}$	$\frac{26875}{104976}$	$\frac{3419375}{7558272}$	$\frac{115625}{472392}$	$\frac{347897}{7558272}$
2	0	$\frac{125}{729}$	$\frac{7625}{17496}$	$\frac{7375}{23328}$	$\frac{5359}{69984}$
3	0	0	$\frac{15625}{46656}$	$\frac{11375}{23328}$	$\frac{8281}{46656}$
4	0	0	0	$\frac{125}{216}$	$\frac{91}{216}$
5	0	0	0	0	1

Therefore, the desired probability of getting a 'Yahtzee' is

$$P(1 \to 5) = \frac{347897}{7558272} = \boxed{4.60\%}$$

Getting k consecutive successes in n Bernoulli trials

Now what if I want to get k consecutive heads in some coin flips?

Problem 80. I flip a coin repeatedly until I get 5 consecutive heads. What is the probability that I need 30 flips or less?

(Difficulty level: 8)

Solution 80. Let the states be the streak of heads I am currently on. There are 6 states, which are 0, 1, 2, 3, 4, 5. When I flip a tail at any times, my streak of heads is reset to 0 , and when I flip 5 heads in a row, my goal is accomplished so I stop the process. Therefore, state 5 is an absorbing state.

We can construct a transition matrix A as follows:

from / to	0	1	2	3	4	5
0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0
1	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0
2	$\frac{1}{2}$	0	0	$\frac{1}{2}$	0	0
3	$\frac{1}{2}$	0	0	0	$\frac{1}{2}$	0
4	$\frac{1}{2}$	0	0	0	0	$\frac{1}{2}$
5	0	0	0	0	0	1

The top right entry of A^{30} is our desired probability. Using a computer to calculate it:

$$P(\text{5 consecutive heads in 30 flips or less}) = (A^{30})_{0,5} = \boxed{\frac{395\,386\,763}{1\,073\,741\,824}}\,.$$

4 Expected value

Sometimes, the outcomes of an experiment are different real numbers, and we want to find the value of an outcome on average. For example, when we are throwing a dice, we may want to know what the average value of the number obtained is. This is where the concept of **expected value** comes in.

II

References

[1] H. Pishro-Nik, "Introduction to probability, statistics, and random processes," 2014. [Online]. Available: https://www.probabilitycourse.com

[2] P. Gorroochurn, *Classic Problems of Probability.* Wiley, 2012.

[3] Brilliant, "Additional practice: Probability," 2022. [Online]. Available: https://brilliant.org/practice/probability-by-outcomes/?p=2

[4] New Senior Secondary Mathematics in Action, *Mathematics textbook 5B Ch.11 - More about Probability.* New Senior Secondary Mathematics in Action, 2012.

[5] Dr. Jeremy Orloff / Jonathan Bloom, "18.05 introduction to probability and statistics problem set 1, spring 2014," 2014. [Online]. Available: https://ocw.mit.edu/courses/18-05-introduction-to-probability-and-statistics-spring-2014/7d6fc9de419b9176934b483146ad96a4_MIT18_05S14_ps2.pdf

[6] ——, "18.05 introduction to probability and statistics problem set 1, spring 2014," 2014. [Online]. Available: https://ocw.mit.edu/courses/18-05-introduction-to-probability-and-statistics-spring-2014/8c8924a12f84f1817546f557090eb6bf_MIT18_05S14_ps2_solutions.pdf

[7] ——, "18.05 introduction to probability and statistics problem set 1, spring 2014," 2014. [Online]. Available: https://ocw.mit.edu/courses/18-05-introduction-to-probability-and-statistics-spring-2014/ae4afab20dd6bfe9ac596eb04860488b_MIT18_05S14_ps1.pdf

[8] ——, "18.05 introduction to probability and statistics problem set 1, spring 2014," 2014. [Online]. Available: https://ocw.mit.edu/courses/18-05-introduction-to-probability-and-statistics-spring-2014/dcd3abc5eb643e1a0d4874b61e3979f1_MIT18_05S14_ps1_solutions.pdf

[9] Proof_Wiki, "Inclusion-exclusion principle," 2022. [Online]. Available: https://proofwiki.org/wiki/Inclusion-Exclusion_Principle

[10] Brilliant, "Derangements wiki," 2022. [Online]. Available: https://brilliant.org/wiki/derangements/

[11] DeriveIt, "Representing e^x as an infinite series," 2022. [Online]. Available: https://www.deriveit.net/calculus/using_euler's_number/e_series2.html

[12] J. M. ain't a mathematician, "Answer: I have a problem understanding the proof of rencontres numbers (derangements)," 2011. [Online]. Available: https://math.stackexchange.com/questions/83380/i-have-a-problem-understanding-the-proof-of-rencontres-numbers-derangements

[13] J. Tanton, "Arrangements and derangements," 2010. [Online]. Available: https://www.math.emory.edu/~rg/derangements.pdf

[14] Brilliant, "Additional practice: Probability: Principle of inclusion and exclusion," 2022. [Online]. Available: https://brilliant.org/practice/principle-of-inclusion-and-exclusion-level-4-5/?p=5

[15] Project Euler, "Problem 205: Dice game," 2008. [Online]. Available: https://projecteuler.net/problem=205

[16] Maths_Rocks, "Probability of sum to be divisible by 7," Mathematics Stack Exchange. [Online]. Available: https://math.stackexchange.com/questions/1680976/probability-of-sum-to-be-divisible-by-7

[17] J. Gravner, "Twenty problems in probability," 2011. [Online]. Available: https://www.math.ucdavis.edu/~gravner/MAT135A/resources/chpr.pdf

[18] M. Penn, "Number theory: The division algorithm," YouTube. [Online]. Available: https://www.youtube.com/watch?v=qEaxFxUK-es&list=PL22w63XsKjqwAgBzVFVqZNMcVKpOOAA7c&index=2&ab_channel=MichaelPenn

[19] D. Chua, "Numbers and sets (ch.3, p.12," 2014. [Online]. Available: https://dec41.user.srcf.net/notes/IA_M/numbers_and_sets.pdf

[20] Wikipedia, "Bézout's identity," 2022. [Online]. Available: https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity

[21] user2345215, "Answer: Prove that (ma, mb) = |m|(a, b) [gcd & lcm distributive law]," Mathematics Stack Exchange. [Online]. Available: https://math.stackexchange.com/q/705884

[22] Proof_Wiki, "Product of gcd and lcm," 2022. [Online]. Available: https://proofwiki.org/wiki/Product_of_GCD_and_LCM

[23] J. C. Santos, “Answer: $d_1, d_2 \mid n \iff \operatorname{lcm}(d_1, d_2) \mid n$ [lcm universal property],” Mathematics Stack Exchange. [Online]. Available: https://math.stackexchange.com/q/2322127

[24] Shambhala, “Does lcm have distributive property of multiplication?” Mathematics Stack Exchange. [Online]. Available: https://math.stackexchange.com/q/4293631

[25] J. Hefferon, “Elementary number theory,” 2003. [Online]. Available: https://joshua.smcvt.edu/numbertheory/book.pdf

[26] Pedro (https://math.stackexchange.com/users/23350/pedro), “What’s the proof that the euler totient function is multiplicative?” Mathematics Stack Exchange. [Online]. Available: https://math.stackexchange.com/questions/192452/whats-the-proof-that-the-euler-totient-function-is-multiplicative

[27] B. Dubuque, “Answer: Show $gcd(a_1, a_2, a_3, \ldots, a_n)$ is the least positive integer that can be expressed in the form $a_1x_1 + a_2x_2 + \ldots + a_nx_n$,” Mathematics Stack Exchange. [Online]. Available: https://math.stackexchange.com/q/718833

[28] ——, “$\gcd(a, b, c) = \gcd(\gcd(a, b), c)$ [associative law for gcd, lcm],” Mathematics Stack Exchange. [Online]. Available: https://math.stackexchange.com/q/1189430

[29] Project Euler, “Problem 72: Counting fractions,” 2008. [Online]. Available: https://projecteuler.net/problem=72

[30] ——, “Problem 72: Counting fractions,” 2008. [Online]. Available: https://en.wikipedia.org/wiki/Euler%27s_totient_function

[31] D. Ma, “Euler’s phi function is multiplicative,” 2015. [Online]. Available: https://exploringnumbertheory.wordpress.com/2015/11/13/eulers-phi-function-is-multiplicative/

[32] Wikipedia, “Euler’s totient function.” [Online]. Available: https://en.wikipedia.org/wiki/Euler’s_totient_function

[33] M. Goemans, “Generating functions (18.310 lecture notes),” 2015. [Online]. Available: https://math.mit.edu/~goemans/18310S15/generating-function-notes.pdf

[34] 3Blue1Brown, “Olympiad level counting: How many subsets of 1,...,2000 have a sum divisible by 5?” YouTube. [Online]. Available: https://www.youtube.com/watch?v=bOXCLR3Wric&t=1085s&ab_channel=3Blue1Brown

[35] Brilliant, “De moivre’s theorem,” 2022. [Online]. Available: https://brilliant.org/wiki/de-moivres-theorem/

[36] N. Verma, “Multiples of an integer modulo another integer,” 2022. [Online]. Available: https://mathsanew.com/articles/multiples_of_an_integer_modulo_another_integer.pdf

[37] HarryPotter5777, “Comment: Simple solution to ”number of subsets of 1..2000 that sum up to a multiple of 5”,” Reddit. [Online]. Available: https://www.reddit.com/r/mathriddles/comments/uzmhzz/comment/iac4b74/?utm_source=share&utm_medium=web2x&context=3

[38] Brian M. Scott, “Answer: Exponential generating function for derangements,” Mathematics Stack Exchange. [Online]. Available: https://math.stackexchange.com/questions/240357/exponential-generating-function-for-derangements

[39] Reducible, “5 simple steps for solving any recursive problem,” YouTube. [Online]. Available: https://www.youtube.com/watch?v=ngCos392W4w&list=PL5GtIFjsbjJ-qhAMsp_CTb3UZjZ-H-YJR&index=16&t=1127s&ab_channel=Reducible

[40] Columbia University, “Gambler’s ruin problem,” 2022. [Online]. Available: http://www.columbia.edu/~ks20/FE-Notes/4700-07-Notes-GR.pdf

[41] N. Nerd, “Markov chains clearly explained! part - 1,” 2020. [Online]. Available: https://www.youtube.com/watch?v=i3AkTO9HLXo&t=7s&ab_channel=NormalizedNerd

[42] V. Mukhachev, “Matrix calculator,” 2022. [Online]. Available: https://matrixcalc.org/

[43] 3Blue1Brown, “Linear combinations, span, and basis vectors | chapter 2, essence of linear algebra,” YouTube. [Online]. Available: https://www.youtube.com/watch?v=k7RM-ot2NWY&list=PLZHQObOWTQDPD3MizzM2xVFitgF8hE_ab&index=2&ab_channel=3Blue1Brown

[44] ——, "Eigenvectors and eigenvalues | chapter 14, essence of linear algebra," YouTube. [Online]. Available: https://www.youtube.com/watch?v=PFDu9oVAE-g&list=PLZHQObOWTQDPD3MizzM2xVFitgF8hE_ab&index=15&ab_channel=3Blue1Brown

[45] A. Magidin, "Answer: How to prove that eigenvectors from different eigenvalues are linearly independent," Mathematics Stack Exchange. [Online]. Available: https://math.stackexchange.com/q/29374

[46] I. Math, "Eigenbasis and diagonalization," 2022. [Online]. Available: https://intuitive-math.club/linear-algebra/eigenbasis

[47] R. Fewster, "Chapter 8: Markov chains (p.157)," 2014. [Online]. Available: https://www.stat.auckland.ac.nz/~fewster/325/notes/ch8.pdf

[48] ——, "Chapter 2: Probability (p.28)," 2014. [Online]. Available: https://www.stat.auckland.ac.nz/~fewster/325/notes/ch2.pdf

[49] Art of Problem Solving, "2020 amc 10a problems/problem 13," 2020. [Online]. Available: https://artofproblemsolving.com/wiki/index.php/2020_AMC_10A_Problems/Problem_13

[50] A. D. Sole, "18.445 problem set 3. solutions," 2011. [Online]. Available: https://math.mit.edu/classes/18.445/18445all/pset-solutions/Pset3_solutions.pdf

[51] Cornell University, "Yahtzee," 2006-2007. [Online]. Available: http://pi.math.cornell.edu/~mec/2006-2007/Probability/Yahtzee.pdf