MATHEMATICS 300 — FALL 2017

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

PART X

Contents

21 Finite sets

There are two kinds of sets: finite sets and infinite sets.

Finite sets are much easier to think about and study, but infinite sets are much more numerous, and much more interesting, because they have many strange and surprising properties.

Since finite sets are easier to understand and work with, we will discuss them first. And then, in the next section, we will study infinite sets.

21.1 What is a finite set? What is an infinite set?

You probably think you know the answer to these questions. But many people who think they know the answer will say, when asked, things like

- A finite set is a set that has a finite number of members.
- A finite set is a set that has finitely many members.
- A finite set is a set that has n members, for some natural number n.
- A finite set is a bounded set.

But ***none of this answers is acceptable***.

If you answer that “a finite set is a set that has a finite number of members”, or “a finite set is a set that has finitely many members”, then these answers are either circular, or presuppose that we know what “having a finite number of members”, or “having finitely many members”, means (as distinct from “being a finite set”):

- If you think that “having a finite number of members” is just another way of saying “is finite”, then you are just saying that “a set is finite if it is a finite set”, which is a circular, totally useless, statement.
- If you think that “having a finite number of members” does not just mean the same as “is finite”, then you have to tell me what it means.

If you answer that “a finite set is a set that has n members, for some natural number n”, then you still have to tell me what that means. You probably think that the meaning is clear, but if it is so clear then it should be possible to give a precise definition.

And if you answer that "a finite set is a bounded set", then I have two serious problems with that.

1. First of all, *sets can be sets of any kinds of objects.* For example, we can have a set of giraffes, or a set of galaxies, or a set of molecules, or a set of integers, or a set of real numbers, or a set of sets[1], or a set of matrices, or a set of lists, or even a very heterogeneous set that has members of lots of different kinds: some real numbers, some sets, some cows, several stars, a number of movies, five books, a chicken, a guitar, and your house. And I haven't the faintest idea of what it might possibly mean for such a set to be "bounded".

   The last time I looked, the definition of "bounded set" says that "if X is a subset of $\mathbb{R}$, then X is <u>bounded</u> if $(\exists C \in \mathbb{R})(\forall x \in X)|x| \leq C$." So, according to this definition, it makes sense for a set of real numbers to be "bounded", but it doesn't make sense for other sets, such as, for example, a set of giraffes, to be "bounded".

2. Second, even if we were talking about sets of real numbers, "bounded" and "finite" are two totally different concepts. For example, the closed interval $[0, 1]$ is bounded but infinite, as I shall show you in subsection 21.1.5.

21.1.1 Our intuitions about what a finite set is and about the number of members of a set can be contradictory

We all have an intuition of what a finite set is, and our intuition tells us all kinds of things. But not all these intuitions are correct. And many of these intuitions are not precise. And this causes problems, because when we do not have a precise understanding of what something means, we cannot prove or disprove statements about this thing, and if our intuition leads us to contradictory beliefs then we do not know how to decide which belief is right.

[1] For some mysterious reason, some students seem to think that "a set cannot be a member of another set". ***Where on Earth did they get that idea?*** Nobody has ever said that "a set cannot be a member of another set". Furthermore, we have discussed the power set $\mathcal{P}(A)$ of a set A. And, you see, $\mathcal{P}(A)$ is a set whose members are sets!

21.1.2 Our intuitions can be contradictory: Hilbert's hotel and Galileo's paradox

Here is an example of two things that our intuitions tell us must be true and yet, as we will show, they contradict each other:

Intuitive idea No. 1: *Suppose that two sets A and B are "perfectly matched", or "perfectly paired", in the sense that*

- *To each member a of A there corresponds a member $m(a)$ of B, called "the member of B matched with a", in such a way that*
  - *(i) every member a of A is matched to one and only one member $m(a)$ of B,*
  - *(ii) every member b of B is the member of B matched with one and only one a of A. (That is, $(\forall b \in B)(\exists! a \in A) m(a) = b$.)*

Then A and B have the same number of members.

Example 54. Suppose you see in a theater that there are lots of seats and lots of people, and (i) every person is seated, (ii) every seat is occupied by one person. Then you can conclude, ***without having to count***, that the number of seats is equal to the number of people. ***You do not need to count and find out how many people and how many chairs there are, in order to know that the two numbers are the same.*** All you need is to observe that the set of people and the set of seats are perfectly matched: every person occupies a seat, and every seat is occupied by a person, □

Example 55. Suppose you see several toys and several boxes, and you observe that: (i) every box has a toy in it, (ii) no box has two or more toys, (iii) every toy is in a box.

Then you know, ***without having to count***, that the number of boxes is the same as the number of toys. □

Intuitive idea No. 2: *If we remove one or more members from a set A, then the resulting set B has fewer members than A, not the same number of members as A. And if we add one or more members to a set A, then the resulting set B has more members than A, not the same number of members as A.*

Example 56. Suppose that last night you bought ten oranges, and after that you ate one of those oranges. Then you can be sure that you now have fewer than ten oranges. □

Example 57. If A is the set of all the natural numbers from 1 to $1,000,000$, and you remove from A all the prime numbers, thus producing a set B (so B is the set $\{\, n \in \mathbb{N} : n \leq 1,000,000 \wedge n \text{ is not prime} \,\}$) then you know for sure that B has fewer that $1,000,000$ members, because A has $1,000,000$ members, and B is obtained from A by removing some members of A. ***You do not need to write down the lists of all the members of*** A ***and*** B ***and see how many members*** A ***and*** B ***have in order to arrive at this conclusion.*** □

Example 58. Suppose a hotel is full, in the sense that every room is occupied by at least one guest. Suppose a new person arrives, seeking a room, and this person is not willing to share a room with another guest. Then there is no way that this new guest can be accommodated, because, if n is the number of rooms, in order to accommodate the new guest you would need to have $n+1$ rooms, and the hotel only has n rooms. □

Yet, it turns out that there are situations where these two "intuitively obvious" ideas yield contradictory conclusions, so they cannot both be correct.

Let us take another look at the hotel example.

Hilbert's Hotel

Imagine a hotel with infinitely many rooms, labeled by the natural numbers. That is, there is room 1, room 2, room 3, and so on, one room for each natural number. Suppose the hotel is full, in the sense that all the rooms are occupied.

Now suppose a new guest arrives, and asks for a room. You would think that it is not possible to accommodate this guest. But this is not true. It is easy to accommodate the new guest! All the hotel has to do is this: move the guest or guests that were occupying room 1 to room 2, move the guest or guests that were occupying room 2 to room 3, move the guest or guests that were occupying room 3 to room 4, and so on. This frees up room 1, and the new guest can be given that room.

To put it somewhat differently: let[a] $\aleph_0$ be the number of rooms in the hotel. To give a room to a new guest the hotel needs to have $\aleph_0 + 1$ rooms. And the hotel "only" has $\aleph_0$ rooms. However, the hotel *does* have enough rooms to accommodate the new guest, so it appears that $\boxed{\aleph_0 + 1 = \aleph_0}$.

This clearly contradicts Intuitive idea No. 2: We added more members to the set of guests, and the new set of guests still "has the same number of members" as the old set, not a larger number.

[a] "$\aleph$" is the Hebrew letter "aleph". George Cantor, the founder of set theory, introduced the notation $\aleph_0$, $\aleph_1$, $\aleph_2$, etc., for infinite cardinals. And this notation is widely used by mathematicians today.

And here is another example of a similar situation.

Galileo's paradox

Suppose A is the set of all natural numbers, that is, $A = \mathbb{N}$. Suppose B is the set of all the natural numbers that are squares, so the members of B are 1, 4, 9, 16, 25, and so on. (That is: $B = \{n \in \mathbb{N} : (\exists m \in \mathbb{N})m^2 = n\}$.)
Then it is clear that B is "much smaller than A", because B is the result of removing from A a large number of members of A. (Actually, to obtain B from A we have to remove from A all the natural numbers that are not squares, that is, the numbers $2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, 18, \ldots$. It is clear that in this process we are removing "most" of the natural numbers: we are only leaving in the squares, which are "very few". For example, out of the first 100 natural numbers, only 10 are squares, so we are removing 90 numbers and keeping 10.) So,

according to intuition No. 1, B ***has fewer members than*** A***.***

And yet, we can construct a "perfect matching" between A and B by pairing each member n of A with its square n^2, which is a member of B. Under this correspondence, each member of A is matched to one and only one member of B, and each member of B is matched to one and only one member of A. So

according to intuition No. 2, B ***has the same number of members as*** A***.***

These two conclusions are contradictory. So one of them must be wrong.

21.1.3 Review of the definition of "finite set"

We begin by recalling some definitions.

First of all, we recall that "$\mathbb{N}_n$" stands for "the set of all natural numbers k such that $k \leq n$". So, for example,

- $\mathbb{N}_0$ is the empty set;
- $\mathbb{N}_1$ is the set $\{1\}$,
- $\mathbb{N}_2$ is the set $\{1, 2\}$,
- $\mathbb{N}_3$ is the set $\{1, 2, 3\}$,

. . . .

- $\mathbb{N}_{15}$ is the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$.

We now review the definitions of "finite set" and "infinite set".

Definition 58. If S is a set and $\mathbf{a} = (a_j)_{j=1}^n$ is a finite list, we say that $\mathbf{a}$ is a list of members of S if every entry of $\mathbf{a}$ belongs to S.

In formal language, $\mathbf{a}$ is a list of members of S if

$$(\forall j \in \mathbb{N}_n) a_j \in S\,.$$

Definition 59. If S is a set and $\mathbf{a} = (a_j)_{j=1}^n$ is a finite list, we say that $\mathbf{a}$ is a list of all the members of S if every entry of $\mathbf{a}$ belongs to S and every member of S is an entry of $\mathbf{a}$. .

In formal language, $\mathbf{a}$ is a list of all the members of S if

$$(\forall j \in \mathbb{N}_n) a_j \in S \wedge (\forall x \in S)(\exists j \in \mathbb{N}_n) x = a_j\,.$$

Definition 60. If $\mathbf{a} = (a_j)_{j=1}^n$ is a finite list, the set of entries of $\mathbf{a}$ is the set $\text{Set}(\mathbf{a})$ given by

$$\text{Set}(\mathbf{a}) = \Big\{\, x : (\exists j \in \mathbb{N}_n) x = a_j \,\Big\}\,.$$

That is, $\text{Set}(\mathbf{a})$ is the set whose members are all the entries of $\mathbf{a}$. □

If should be clear from the above definitions that saying that "$\mathbf{a}$ is a list of all the members of S" is exactly equivalent to saying that "$S = \text{Set}(\mathbf{a})$".

Definition 61. Let S be a set. We say that S is finite if there exists a finite list $\mathbf{a} = (a_j)_{j=1}^n$ such that $\mathbf{a}$ is a list of all the members of S.

In other words, S is finite if and only if there exists a finite list $\mathbf{a} = (a_j)_{j=1}^n$ such that $S = \mathrm{Set}(\mathbf{a})$. □

Definition 62. Let S be a set. We say that S is infinite if S is not finite. □

21.1.4 Examples of finite and infinite sets

Now that we know what a "finite set" is and what an "infinite set" is, we should give some examples of both kinds of sets.

Example 59.

Proposition 1. *If n is a natural number, then the set $\mathbb{N}_n$ is finite.*

Proof. We write a finite list $\mathbf{a} = (a_j)_{j=1}^n$ of all the members of $\mathbb{N}_n$. We define a_j, for $j \in \mathbb{N}_n$, by letting $a_j = j$. Then it is clear that $\mathbf{a}$ is a list of all the members of $\mathbb{N}_n$, because

1. $\mathbf{a}$ is a list of members of $\mathbb{N}_n$, because if $j \in \mathbb{N}_n$ then $a_j \in \mathbb{N}_n$, since $a_j = j$, so every entry of $\mathbf{a}$ is in $\mathbb{N}_n$.

2. $\mathbf{a}$ is a list of *all* the members of $\mathbb{N}_n$, because if $x \in \mathbb{N}_n$ then we may pick $j = x$, and with this choice $j \in \mathbb{N}_n$ and $x = a_j$, so every member of $\mathbb{N}_n$ occurs as an entry of $\mathbf{a}$.

It follows from the definition of "finite set" that $\mathbb{N}_n$ is finite. □

Example 60.

Proposition 2. *The set $\mathbb{N}$ of all natural numbers is infinite.*

Proof.

Suppose $\mathbb{N}$ was finite.

Then we would be able to pick a finite list $\mathbf{a} = (a_j)_{j=1}^n$ which is a list of all the members of $\mathbb{N}$.

Let

$$m = 1 + \sum_{j=1}^{n} a_j \,. \tag{21.1}$$

> Then m is not an entry of $\mathbf{a}$. (Reason: if m was an entry of $\mathbf{a}$ then we would be able to pick an index $i \in \mathbb{N}_n$ such that $m = a_i$. But (21.1) implies that $m > a_i$. So assuming that m is an entry of $\mathbf{a}$ leads to a contradiction.)
>
> But m is an entry of $\mathbf{a}$, because $m \in \mathbb{N}$ and $\mathbf{a}$ is a list of all the members of $\mathbb{N}$.
>
> So m is an entry of $\mathbf{a}$ and m is not an entry of $\mathbf{a}$, and we have reached a contradiction.

So $\mathbb{N}$ is infinite. **Q.E.D.**

Example 61.

Proposition 3. *Every subset of a finite set is finite.*

Proof. Let A be a finite set and let B be a subset of A. We want to prove that B is finite.

If $B = A$ then B is finite, because A is.

So let us assume $B \neq A$.

Let $\mathbf{a} = (a_j)_{j=1}^n$ be a finite list of of all the members of A.

We will construct a new finite list $\mathbf{b} = (b_j)_{j=1}^k$ by removing from $\mathbf{a}$ all the entries that are not in B.

We create the list $\mathbf{b}$ in several steps as follows:

Step 1: Removal of one entry. Since we are assuming that $B \subseteq A$ and $B \neq A$, we can pick a member x_1 of A such that $x_1 \notin B$.

Since $\mathbf{a}$ is a list of all the members of A, there must exist an index $i \in \mathbb{N}_n$ such that $a_i = x_1$.

We then remove the entry a_i, taking care of moving a_{i+1} to the i-th place, a_{i+2} to the $i+1$-th place, and so on.

Precisely, we define a new list $\mathbf{a^{(1)}} = (a_j^{(1)})_{j=1}^{n-1}$ by letting

$$a_j^{(1)} = \begin{cases} a_j & \text{if} \quad j < i \\ a_{j+1} & \text{if} \quad i \leq j \leq n-1 \end{cases} .$$

(So, for example, if we want to remove the entry a_8, we take $a_j^{(1)} = a_j$ for $j = 1, 2, 3, 4, 5, 6, 7$, but then we let $a_8^{(1)} = a_9$, $a_9^{(1)} = a_{10}$, and so on.)

The new list $\mathbf{a^{(1)}}$ has one fewer entry than $\mathbf{a}$, and has exactly the same set of entries as $\mathbf{a}$, except possibly[2] for x_1 (that is, $\text{Set}(\mathbf{a^{(1)}}) = \text{Set}(\mathbf{a})$), or $\text{Set}(\mathbf{a^{(1)}}) = \text{Set}(\mathbf{a}) - \{x_1\}$),

So $\mathbf{a^{(1)}}$ is a list of all the members of a set A_1 which is either A or $A - \{x_1\}$. In particular, $B \subseteq A_1$ and $A_1 \subseteq A$.

If $A_1 = B$, then we take $\mathbf{b} = \mathbf{a^{(1)}}$, and we are done. The list $\mathbf{b}$ is a list of all the members of B, so B is finite.

Removal of all the entries that are not in B. If $B \neq A_1$, then we repeat the removal process (by picking an x_2 such that $x_2 \in A_1$ but $x_2 \notin B$ and removing an entry a_{i_2} such that $A_{i_2} = x_2$), and form a list $\mathbf{a^{(2)}} = (a_j^{(2)})_{j=1}^{n-2}$ which is a list of all the members of a set A_2 such that $B \subseteq A_2$ and $A_2 \subseteq A$.

And we continue in this way, removing one entry at a time, until the process stops,

The process will stop when we get to a list $\mathbf{a^{(r)}}$ that is a list of all the members of a set A_r such that $B = A_r$. And when we get there we can take $\mathbf{b}$ to be $\mathbf{a^{(r)}}$, and then $\mathbf{b}$ is a list of all members of B, so B is finite, and we are done. **Q.E.D.**

Remark 31. Exactly how do we know that this process will stop?

Intuitively, the process has to stop because at every step the length of the list goes down by 1. (That is, $\mathbf{a^{(1)}}$ has length $n-1$, $\mathbf{a^{(2)}}$ has length $n-2$, and so on.) And the lengths cannot keep going down for ever, because if they did so then at the $n+1$-th step we would have a list with a negative length, which is impossible.

Another way to see that the removal process of the proof of Proposition 3 has to stop is to use the well-ordering principle as follows . Let S be the set of all the lengths of all the lists produced by this process. Then S is a set of nonnegative integers. By the well-ordering principle, S has a smallest member s. Then s is a nonnegative integer. and the process must stop at step s. □

Example 62.

Proposition 4. *The union of two finite sets is finite.*

[2] We are not assuming that $\mathbf{a}$ is a list without repetitions. So x_1 could still be an entry of $\mathbf{a}^{(1)}$ even after the entry a_i has been removed. This would be so if there was another index j, different from i, such that $a_j = a_i$,

Proof. Let A, B be finite sets.

Let $\mathbf{a} = (a_j)_{j=1}^n$ be a finite list of of all the members of A, and let $\mathbf{b} = (b_j)_{j=1}^m$ be a finite list of of all the members of B.

Let $\mathbf{c}$ be the concatenation[3] of $\mathbf{a}$ and $\mathbf{b}$. That is, $\mathbf{c} = (c_j)_{j=1}^{m+n}$, where

$$c_j = \begin{cases} a_j & \text{if} \quad j \in \mathbb{N},\, j \leq m \\ b_{j-m} & \text{if} \quad j \in \mathbb{N}.\, m+1 \leq j \leq m+n \end{cases} .$$

Then $\mathbf{c}$ is a finite list of all the members of $A \cup B$. So $A \cup B$ is finite.**Q.E.D.**

Example 63.

Proposition 5. *Let N be a natural number, and let*

$$A_N = \{k \in \mathbb{Z} : |k| \leq N\}\,.$$

Then A_N is a finite set.

Proof. Let $B_N = \{k \in \mathbb{Z} : -k \in \mathbb{N}_N\}$.

Then B_N is a finite set, because we can construct a list $\mathbf{b} = (b_j)_{j=1}^N$ of all the members of B_N by defining $b_j = -j$ for $j \in \mathbb{N}_N$.

Clearly, $A_N = \mathbb{N}_N \cup B_N \cup \{0\}$. So A_N is the union of three finite sets, and Proposition 4 tells us that A_N is finite. **Q.E.D.**

We have already talked about ***bounded sets*** before. Let us recall the definition

Definition 63. A subset A of $\mathbb{Z}$ is bounded if there exists a natural number N such that $(\forall n \in A)|n| \leq N$. □

Example 64.

Proposition 6. *A subset A of $\mathbb{Z}$ is finite if and only if it is bounded.*

Proof. Let A be a subset of $\mathbb{Z}$.

We have to prove two things:

[3] The concatenation of two finite lists $\mathbf{a}$, $\mathbf{b}$, is the list $\mathbf{a}\#\mathbf{b}$ obtained by writing the list $\mathbf{a}$ and then the list $\mathbf{b}$. For example, if $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5)$ and $\mathbf{b} = (b_1, b_2, b_3, b_4)$, then $\mathbf{a}\#\mathbf{b} = (a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4)$. So $\mathbf{a}\#\mathbf{b} = (c_j)_{j=1}^9$, where $c_1 = a_1$, $c_2 = a_2$, $c_3 = a_3$, $c_4 = a_4$, $c_5 = a_5$, $c_6 = b_1$, $c_7 = b_2$, $c_8 = b_3$, and $c_9 = b_4$.

(I) If A is bounded then A is finite.

(II) If A is finite then A is bounded.

Proof of (I). Assume A is bounded. Pick a natural number N such that $|n| \leq N$ for all $n \in A$.

Then A is a subset of the set A_N defined in Example 63. And Proposition 5 tells us that A_N is finite. So Proposition 3 implies that A is finite.

Proof of (I). Assume A is finite.

Let $\mathbf{a} = (a_j)_{j=1}^n$ be a finite list of all the members of A.

Let $N = 1 + \sum_{j=1}^n |a_j|$. Then N is a natural number and $|a_j| \leq N$ for every $j \in n$.

It follows from this that $\boxed{|k| \leq N \text{ for every } k \in A}$. (Reason: if $k \in A$, then $k = a_j$ for some j, because $\mathbf{a}$ is a list of all the members of A.)

So A is bounded. **Q.E.D.**

Example 65.

Proposition 7. *The set $\mathbb{Z}$ of all integers is infinite.*

Proof. We can prove this in lots of different ways. Here are two examples:

- $\mathbb{Z}$ is clearly not bounded. So Proposition 6 tells us that $\mathbb{Z}$ is infinite.
- $\mathbb{N}$ is a subset of $\mathbb{Z}$. If $\mathbb{Z}$ was finite then Proposition 3 would imply that $\mathbb{N}$ is finite. But we know that $\mathbb{N}$ is infinite. **Q.E.D.**

21.1.5 "Finite" is not the same as "bounded"

An example of an incorrect idea students often have is that they confuse the notion of "finite set" with the notion of "bounded set". And yet ***"finite set" is totally different from "bounded set".***

It is true that, for subsets of $\mathbb{Z}$, "bounded" is equivalent to "finite", as we proved in Example 64.

But ***for subsets of*** $\mathbb{R}$ ***the two notions are very different.***

And ***for more general sets (e.g., sets of giraffes, or of galaxies, or of sets, or of lists, or of functions, or of molecules, or of abstract ideas), "finite" is a perfectly meaningful notion but "bounded" is not.***

Let us look at sets of real numbers. In this case, the notions of "bounded set" and "finite set" are both perfectly meaningful, but ***the definitions of "bounded set" and "finite set" are completely different.*** (Just look at them, and you will see.)

And, in case you are not convinced by that, here is an example of a bounded set that is infinite.

Example 66. Let S be the closed interval $[0,1]$, so S is the set of all real numbers x such that $0 \leq x \leq 1$. In formal language,

$$S = \{x \in \mathbb{R} : 0 \leq x \leq 1\}\,.$$

Then S ***is a bounded subset of*** $\mathbb{R}$. Why? Because the definition of "bounded subset of $\mathbb{R}$" says that

(B) If X is a subset of $\mathbb{R}$, we say that X is <u>bounded</u> if there exists a real number C such that $|x| \leq C$ for every $x \in X$.

So the set S is bounded, because of the following simple argument:

> Let $C = 1$.
> Let x be an arbitrary member of S.
> Then $0 \leq x \leq 1$.
> So $|x| \leq 1$, i.e., $|x| \leq C$.
> Since we have shown that $|x| \leq C$ for arbitrary $x \in S$, we can conclude from Rule $(\forall_{prove})$ that $(\forall x \in S)\,|x| \leq C\,.$
> So, by Rule $\exists_{use}$, $(\exists C \in \mathbb{R})(\forall x \in S)\,|x| \leq C\,.$
> So S is bounded. **Q.E.D.**

But S ***is an infinite set.*** Why? This can be proved in a number of ways. Here is one.

We will prove that the open interval $]0,1[$, that is, the set of all real numbers x such that $0 < x < 1$, is infinite. This will imply that the closed interval $[0,1]$ is infinite as well, because if $[0,1]$ was finite then its subset $]0,1[$ would be finite as well.

To prove that $]0,1[$ is infinite, we assume it is finite and derive a contradiction.

Assume that $]0,1[$ is a finite set. Let $\mathbf{a} = (a_j)_{j=1}^{n}$ be a finite list of all the members of $]0,1[$,

Then we may pick an index $i \in \mathbb{N}_n$ such that a_i is the largest of all the a_j, that is, $a_i \geq a_j$ for every $j \in \mathbb{N}_n$.

Then $a_i \in]0,1[$, because $\mathbf{a}$ is a list of members of $]0,1[$. Therefore $0 < a_j < 1$. Let $x = \frac{1}{2}(a_i + 1)$. Then $0 < x < 1$. (Reason: $0 < a_i < 1$. So $0 < a_j + 1 < 2$, and then $0 < \frac{1}{2}(a_j + 1) < 1$, so $0 < x < 1$.)

So $x \in]0,1[$. But x cannot be an entry of $\mathbf{a}$, because $x > a_i$. (Reason: $1 > a_i$, so $1 + a_i > 2a_i$, and then $\frac{1}{2}(1 + a_i) > a_i$, i.e., $x > a_i$.)

So $\mathbf{a}$ is not a list of all the members of $]0,1[$. But $\mathbf{a}$ is a list of all the members of $]0,1[$. So we got a contradiction. □

Problem 45. *Many students seem to think that "finite" means the same as "bounded". The previous example should have persuaded everybody that this is a mistaken idea. The purpose of this problem is to reinforce this, by having you prove that some important sets are bounded and infinite.*

In this problem, we use the following terminology and notations:

- If a, b are real numbers, then
  - The open interval from a to b is the set $]a,b[$ given by
  $$]a,b[= \{x \in \mathbb{R} : a < x < b\},$$
  - The closed interval from a to b is the set $[a,b]$ given by
  $$[a,b] = \{x \in \mathbb{R} : a \le x \le b\},$$

Notice that

- If $a > b$ then both sets $]a,b[$ and $[a,b]$ are empty.
- If $a = b$ then $]a,b[$ is empty and $[a,b]$ is $\{a\}$, the singleton of a, so $[a,b]$ consists of exactly one point.

Prove that if a, b are real numbers such that $a < b$ then the sets $]a,b[$, $[a,b]$ are both bounded and infinite. □

Remark 32. You have probably seen open intervals before, but the name for them was "(a,b)" rather than "$]a,b[$". I am using "$]a,b[$" here because

1. I think this notation is nicer than "(a,b)".
2. I do not want the interval $]a,b[$ to be confused with the ***ordered pair*** (a,b), so I prefer not to use "(a,b)" for the open interval. □

Problem 46. A subset D of $\mathbb{R}$ is said to be dense in $\mathbb{R}$ if every nonempty open interval $]a,b[$ has a nonempty intersection with D. In other words, D is dense in $\mathbb{R}$ if for every pair a,b of real numbers such that $a<b$ there exists a member x of D such that $a<x<b$. (In formal language: D is dense in $\mathbb{R}$ if $(\forall a\in\mathbb{R})(\forall b\in\mathbb{R})\Big(a<b\Longrightarrow(\exists x\in D)a<x<b\Big)$.)

Prove that if D is a dense subset of $\mathbb{R}$ and a,b are real numbers such that $a<b$ then the sets $]a,b[\cap D$, $[a,b]\cap D$ are infinite.

NOTE: (You don't need to know this to do the problem, but it's good to know.) Two important examples of subsets of $\mathbb{R}$ that are dense in $\mathbb{R}$ are (a) the set $\mathbb{Q}$ of all rational numbers, (b) the set $\mathbb{I}$ of all irrational numbers. This will be proved in subsection 21.1.6 □

Problem 47. If n is a natural number, and a, b are two integers, we say that a and b are congruent modulo n if $a-b$ is divisible by n.

We write "$a\equiv_n b$" to indicate that a and b are congruent modulo n. (For example, the following sentences are true: $23\equiv_4 7$, $32\equiv_{17} 15$, $-5\equiv_7 9$, $729\equiv_3 0$, $\sim 33\equiv_3 2$, $\sim 444\equiv_2 1$.)

Prove that there are infinitely many primes that are congruent to 3 modulo 4. (That is, prove that the set of all natural numbers n such that $n\equiv_4 3$ and n is prime is an infinite set.)

NOTE: Here are some examples of primes that are congruent to 3 modulo 4: 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103. The result you are asked to prove says that this list can be continued indefinitely, and never stops.

Here is a guided list of the steps for your proof.

1. First, you should prove that every integer is congruent modulo 4 to one of the integers 0, 1, 2, 3.

2. Next, you should conclude from the previous step that every odd integer is congruent modulo 4 to 1 or 3.

3. Next, you should prove that every prime number other than 2 is odd.

4. Next, you should conclude from the above that every prime number other than 2 is congruent to 1 or to 3 modulo 4.

5. Then you should show that:

   (a) If a,b,c,d are integers, n is a natural number, and $a\equiv_n b$ and $c\equiv_n d$, then $a+c\equiv_n b+d$ and $ac\equiv_n bd$.

(b) As a special case of the above result:

  i. The product of two integers that are congruent to 1 modulo 4 is congruent to 1 modulo 4.

  ii. The product of two integers that are congruent to 3 modulo 4 is congruent to 1 modulo 4.

  iii. The product of an integer that is congruent to 3 modulo 4 and an integer that is congruent to 1 modulo 4 is congruent to 3 modulo 4.

(c) If a natural number n is ≥ 2 and is congruent to 3 modulo 4, then n has a prime factor that is congruent to 3 modulo 4.

6. And now, finally, you should be able to prove the desired conclusion as follows:

   (a) Let $\mathbf{p} = (p_j)_{j=1}^{r}$ be a list of all the primes that are congruent to 3 modulo 4, except for 3. (That is: let S be the set of all natural numbers n such that n is prime, $n \neq 3$, and $n \equiv_4 3$. Let $\mathbf{p}$ be a list of all the members of S.)

   (b) Let
$$M = 3 + 4\prod_{j=1}^{r} p_j \,.$$

   (c) Prove that M is not divisible by 3.

   (d) Prove that M has a prime factor q such that $q \equiv_4 3$.

   (e) Prove that q cannot be equal to 3.

   (f) Prove that q cannot be an entry of the list $\mathbf{p}$, and get a contradiction from this.

Problem 48. ***Prove*** that there are infinitely many primes that are congruent to 5 modulo 6. (That is, prove that the set of all natural numbers n such that $n \equiv_6 5$ and n is prime is an infinite set.)

NOTE: Here are some examples of primes that are congruent to 5 modulo 6: 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101. The result you are asked to prove says that this list can be continued indefinitely, and never stops.)

HINT: Follow a strategy similar to the one you used for the previous problem. □

21.1.6 A couple of facts about rational and irrational numbers; the Archimedean principle and the density of the rationals and the irrationals

The ***Archimedean principle*** is a very important property of the real numbers. It says this:

Fact 1. **(The Archimedean principle)** *If x is an arbitrary real number then there exists a natural number n usch that $x < n$.* □

This is one of the basic facts about the real numbers that, in a formal development of the theory, would either be taken for granted as a starting point for the theory, or would be proved from other basic facts, such as the completeness axiom.

For us, here, the Archimedean principle is just something we will accept. And it should not be surprising to you. You know that

(DE) *Every positive real number r can be written as "$n, d_1d_2d_3\dots$", where n is a nonnegative integer and $d_1, d_2, d_3, \dots$ are digits.*

(The "digits" are the members of the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.)

For example,

$$\sqrt{2} = 1.4142135623730950488016887242096980785696718753769480 73\dots,$$

and

$$\pi = 3.14159265358979323846264338327950288419716939937510582097 4\dots$$

Remark 33. You can find $\sqrt{2}$ with 10 million digits in

https://apod.nasa.gov/htmltest/gifcity/sqrt2.10mil

and one million digits of π in

https://www.angio.net/pi/digits/pi1000000.txt □

Since you can write your real number x as "$n, d_1d_2d_3\dots$", it is clear that $x < n + 1$. And, since every positive real number x can be written that way, and every nonpositive real number x satisfies $x < 1$, we seem to have actually proved the Archimedean principle.

This should at least convince you that the Archimedean principle is true.

But what we have said is not truly a proof, for the following reason: ***I haven't told you how to prove statement (DE), that is, that every positive real number r has a decimal expansion.*** And the fact is, in order to prove (DE) you need to use the Archimedean principle. So the Archimedean principle "comes first", and the argument I gave you to "prove" it is circular.

But my goal was not give you a proof. It was just to convince you that the Archimedean principle is true. And I hope I have achieved that.

Here is how you can use the Archimedean principle to prove, for example, the results of Problem 46.

Definition 64. A subset D of $\mathbb{R}$ is said to be dense in $\mathbb{R}$ if every nonempty open interval $]a, b[$ has a nonempty intersection with D. In other words, D is dense in $\mathbb{R}$ if or every pair a, b of real numbers such that $a < b$ there exists a member x of D such that $a < x < b$.

In formal language: D is dense in $\mathbb{R}$ if

$$(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})\Big(a < b \Longrightarrow (\exists x \in D)a < x < b\Big)\,.$$

In the following theorem, we prove that two important subsets of $\mathbb{R}$ are dense in $\mathbb{R}$. These are two sets already known to you: the set $\mathbb{Q}$ of all rational numbers, and the set $\mathbb{I}$ of all irrational numbers.

Recall that

$$\mathbb{Q} = \Big\{ x \in \mathbb{R} : (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})\Big(n \neq 0 \wedge x = \frac{m}{n}\Big) \Big\}\,.$$

And, clearly,

$$\mathbb{I} = \mathbb{R} - \mathbb{Q}\,,$$

i.e.,

$$\mathbb{I} = \{x \in \mathbb{R} : x \notin \mathbb{Q}\}\,.$$

Theorem 73. *The sets $\mathbb{Q}$ and $\mathbb{I}$ are dense in $\mathbb{R}$.*

Proof. Let us first prove that $\mathbb{Q}$ is dense in $\mathbb{R}$.

We have to prove that if if $a, b \in \mathbb{R}$ and $a < b$, then the set $]a, b[\cap\mathbb{Q}$ is nonempty.

Idea of the proof. *It is a very simple idea: we subdivide the real line $\mathbb{R}$ into intervals of length $\frac{1}{n}$. The subdivision points are the points $\frac{k}{n}$, $k \in \mathbb{Z}$.*

(That is, we divide $\mathbb{R}$ *into the intervals* $[0,\frac{1}{n}]$, $[\frac{1}{n},\frac{2}{n}]$, $[\frac{2}{n},\frac{3}{n}]$, $[\frac{3}{n},\frac{4}{n}]$, $\ldots$, *and also the intervals* $[-\frac{1}{n},0]$, $[-\frac{2}{n},-\frac{1}{n}]$, $[-\frac{3}{n},-\frac{2}{n}]$, $\ldots$.*) And we choose* n *so large that* $\frac{1}{n} < b-a$. *Then, since the interval* $]a,b[$ *is longer than* $\frac{1}{n}$, *the interval* $]a,b[$ *has to contain an endpoint of one of these intervals, and this endpoint will be* $\frac{k}{n}$ *for some* $k \in \mathbb{Z}$, *that is, a rational number. And that will give us a rational number belonging to* $]a,b[$. *The only problem with this idea is this: how do we find* k? *The obvious way is to go from left to right, starting far to the left of* a, *with a point* $\frac{i}{n}$ *(with* $i \in \mathbb{Z}$, *of course) far to the left of* a, *and then make small jumps to the right, going to to* $\frac{i+1}{n}$, $\frac{i+2}{n}$, *and so, until we go past* a *for the first time. Then we will have found* k, *the smallest of all integers* i *such that* $\frac{i}{n} > a$. *And then* $\frac{k}{n}$ *will have to be* $< b$, *because if* $\frac{k}{n}$ *was greater than or equal to* b *then in the jump from* $\frac{k-1}{n}$ *to* $\frac{k}{n}$ *we would have jumped from* $\frac{k-1}{n}$, *which is to the left of* a, *to* $\frac{k}{n}$, *which is to the right of* b, *so we would have made a jump of length* $\frac{1}{n}$ *and jumped over an interval of length* $b-a$, *which is longer than* $\frac{1}{n}$.

But there are two problems with this approach: How do we find $n \in \mathbb{N}$ *such that* $\frac{1}{n} < b-a$? *And how do we find* k? *The following proof takes care of these key issues. And, as you will see, the Archimedean principle is essential. And it will be used twice.*

Using the Archimedean principle, we find a natural number n such that

$$\frac{1}{n} < b-a\,. \tag{21.2}$$

(The Archimedean principle says that there exists a natural number n such that $\frac{1}{b-a} < n$. Then, using Rule $\exists_{use}$, we pick one. Then the fact that $\frac{1}{b-a} < n$ implies the inequality $\frac{1}{n} < b-a$.)

Next, we look at the numbers $\frac{i}{n}$, for all integers i. One of these numbers must be larger than a. (Reason: The Archimedean principle tells us that there exists a natural number m such that $a < m$. Using Rule $\exists_{use}$, pick one such m. Then $a < m = \frac{mn}{n}$. So, if we take $i = mn$, we see that $i \in \mathbb{Z}$ and $a < \frac{i}{n}$.)

So, if we let S be the set of all integers i such that $\frac{i}{n} > a$, the set S is nonempty.

Next, we show that S is bounded below. (Recall that a subset X of $\mathbb{R}$ is <u>bounded below</u> if $(\exists C \in \mathbb{R})(\forall x \in X)x \geq C$.)

For this purpose, observe that if $k \in S$ then $a < \frac{k}{n}$, so $k \geq na$. So, if we take C to be na, we see that $(\forall k \in S)k \geq C$. So S is indeed bounded below.

Next, we want to prove that there exists an integer N such that

$$(\forall k \in S)k \geq N\,. \tag{21.3}$$

Using the Archimedean principle, we find an integer W such that $-C < W$. Then $C > -W$. Take $N = -W$. Then $k \geq C$ for every $k \in S$, and $C > N$. So $k \geq N$ for every $k \in S$. So (21.3) holds.

In one of the previous homework problems, we defined the set $\mathbb{Z}_{\geq q}$, for each integer q, to be the set of all integers that are greater than or equal to q. Then (21.3) tells us that

$$S \subseteq \mathbb{Z}_{\geq N}\,.$$

Also, we proved in the previous homework problem that *if $M \in \mathbb{Z}$ and X is a nonempty subset of $\mathbb{Z}_{\geq M}$, then X has a smallest member.*

In our case, N is an integer, and S is a nonempty subset of $\mathbb{Z}_{\geq N}$. So S has a smallest member. Let us call this smallest member s.

Then $s \in \mathbb{Z}$, and $\frac{s}{n} > a$ (because $s \in S$).

On the other hand, $\frac{s-1}{n} \leq a$. (Reason: if $\frac{s-1}{n}$ was $> a$, it would follow that $s - 1 \in S$, contradicting the fact that s is the smallest member of S.)

Finally, I claim that $\frac{s}{n} < b$. The reason for this is as follows:

Suppose that

$$\frac{s}{n} \geq b\,. \tag{21.4}$$

We know that

$$\frac{s-1}{n} \leq a\,,$$

and then

$$-\frac{s-1}{n} \geq -a\,. \tag{21.5}$$

Adding the two inequalities (21.4) and (21.5), we get

$$\frac{s}{n} - \frac{s-1}{n} \geq b - a\,.$$

But

$$\frac{s}{n} - \frac{s-1}{n} = \frac{1}{n}\,.$$

So

$$\frac{1}{n} \geq b - a\,. \tag{21.6}$$

> But we have chosen n precisely such that $\frac{1}{n} < b - a$. So we got a contradiction.

So we have proved that $\frac{s}{n} < b$.
Hence, if we let $r = \frac{s}{n}$, the rational number r satisfies $a < r < b$.
So $r \in]a, b[\cap \mathbb{Q}$.
Therefore the set $]a, b[\cap \mathbb{Q}$ is nonempty, and this completes the proof that $\mathbb{Q}$ is dense in $\mathbb{R}$.

Now we prove that $\mathbb{I}$ is dense in $\mathbb{R}$.

Let a, b be arbitrary real numbers such that $a < b$.
We know that $\mathbb{Q}$ is dense in $\mathbb{R}$. So we can pick a rational number r such that $a < r < b$.
Using again the fact that $\mathbb{Q}$ is dense in $\mathbb{R}$, we pick a rational number s such that $r < s < b$.
Let

$$u = r + (s - r)\frac{\sqrt{2}}{2}\,.$$

Then $u \in \mathbb{I}$. (Reason: suppose u was rational. Then $\sqrt{2}$ would have to be rational as well, because $\sqrt{2} = 2\frac{u-r}{s-r}$. But we know that $\sqrt{2}$ is irrational as well.)

Furthermore, it is clear that $u > a$, because $r > a$ and $s > r$.
And, finally, $u < b$. (Reason: $\frac{\sqrt{2}}{2} < 1$, so $(s - r)\frac{\sqrt{2}}{2} < s - r$, and then $u = r + (s - r)\frac{\sqrt{2}}{2} < r + (s - r) = s < b$.)

So $a < u < b$, and then $u \in]a, b[\cap \mathbb{Q}$. **Q.E.D.**

Problem 49. A dyadic rational number is a rational number r such that $r = \frac{k}{2^n}$ for some integer k and some natural number n. (So, for example: $\frac{3}{4}$, $\frac{29}{8}$, $\frac{365{,}908}{1{,}024}$, $-\frac{10{,}298{,}635}{2^{234}}$ are dyadic rational numbers.)

Let $\mathbb{D}$ be the set of all dyadic rational numbers.

Prove that $\mathbb{D}$ is dense in $\mathbb{R}$. More precisely:

1. ***Write*** a very short proof (just a few lines), using Theorem 73
2. ***Write*** a proof without using Theorem 73. (That means that you have to write a proof following the same pattern as in the proof we gave of Theorem 73. All you have to do is choose n to be a power of 2.) □

21.2 The cardinality of a finite set

Definition 65. Let $\mathbf{a} = (a_j)_{j=1}^n$ be a finite list. We say that the list $\mathbf{a}$ has no repetitions if no two entries corresponding to different indices can be equal.

In formal language, $\mathbf{a}$ has no repetitions if

$$(\forall i, j \in \mathbb{N}_n)(i \neq j \Longrightarrow a_i \neq a_j)\,. \qquad \Box$$

Definition 66. Let S be a set and let n be a nonnegative integer[4]. We say that S has n members, or that S has cardinality n, if either

1. $S = \emptyset$ and $n = 0$,

or

2. $S \neq \emptyset$, $n \neq 0$, and there exists a finite list $\mathbf{a} = (a_j)_{j=1}^n$ of length n such that
    1. $\mathbf{a}$ is a list of all the members of S,
    2. $\mathbf{a}$ has no repetitions.

In formal language: *S has n members if either $S = \emptyset$ and $n = 0$, or there exists a finite list $\mathbf{a} = (a_j)_{j=1}^n$ of length n such that*

$$\mathrm{Set}(\mathbf{a}) = S \wedge (\forall i, j \in \mathbb{N}_n)(i \neq j \Longrightarrow a_i \neq a_j)\,. \qquad \Box$$

Remark 34. Things get much nicer if we allow also ***the empty list***:

- The empty list is a list of length zero.
- The empty list has no entries.
- If $\mathbf{a}$ is the empty list, then the corresponding set $\mathrm{Set}(\mathbf{a})$ is the empty set.
- And the name of the empty list is $\emptyset$.
- So $\mathrm{Set}(\emptyset) = \emptyset$.
- And it's O.K. to give the same name to the empty list that we gave to the empty set because, when we do things in a more precise way, it will turn out that the empty list ***is*** the empty set.

[4] The ***nonnegative integers*** are the natural numbers together with zero. That is, the nonnegative integers are the members of the set $\mathbb{N} \cup \{0\}$. So $n \in \mathbb{N} \cup \{0\}$" is just another way of saying "n is a nonnegative integer", that is, "n is a natural number or zero".

With this addition of a new list to our supply of finite lists, the definition of "number of members of a set" becomes much simpler: *If S is a set and $n \in \mathbb{N} \cup \{0\}$, we say that $\underline{S \text{ has } n \text{ members}}$ if there exists a list $\mathbf{a}$ of length n without repetitions such that $S = \text{Set}(\mathbf{a})$.* □

It is clear that

Fact 2. *If S is a set that has n members for some $n \in \mathbb{N} \cup \{0\}$, then S is a finite set in the sense of Definition 61.*

To see this, just observe that if S has n members then there must exist a finite list $\mathbf{a} = (a_j)_{j=1}^n$ without repetitions such that $S = \text{Set}(\mathbf{a})$. So, if we forget about the "no repetitions" part, then $\mathbf{a}$ is a finite list of all the members of S, and this tells us that S is finite.

It is also fairly clear that

Fact 3. *If S is a finite set in the sense of Definition 61, then S has n members for some $n \in \mathbb{N} \cup \{0\}$.*

Proof. Suppose S is a finite set. Then there exists a finite list $\mathbf{b} = (b_j)_{j=1}^m$ such that $S = \text{Set}(\mathbf{b})$. In order to prove that S has n members for some $n \in \mathbb{N} \cup \{0\}$, all we need is a finite list $\mathbf{a} = (a_j)_{j=1}^n$ without repetitions such that $S = \text{Set}(\mathbf{a})$. But is is easy to get such a list from the list $\mathbf{b}$. All we have to do is ***remove the repetitions from*** $\mathbf{b}$.

Lemma 7 below tells us that this removal of repetitions is possible. Using the lemma, we find a finite list $\mathbf{a} = (a_j)_{j=1}^n$ without repetitions such that $S = \text{Set}(\mathbf{a})$. And then S has n members. **Q.E.D.**

And here is the lemma that tells us that we can remove the repetitions from a list.

In plain English the lemma says this: *if we start with a finite list* $\mathbf{b}$*, then we can produce a finite list* $\mathbf{a}$ *that has no repetitions and has exactly the same set of entries as* $\mathbf{b}$*. If* $\mathbf{b}$ *already has no repetitions, then* $\mathbf{a}$ *is* $\mathbf{b}$*. Otherwise (that is, if* $\mathbf{b}$ *has repetitions), the length of* $\mathbf{a}$ *is strictly less than the length of* $\mathbf{b}$*.*

Lemma 7. ***(The repetitions removal lemma)*** *Let $\mathbf{b} = (b_j)_{j=1}^m$ be a finite list. Then there exists a finite list $\mathbf{a} = (a_j)_{j=1}^n$ such that*

1. $\text{Set}(\mathbf{a}) = \text{Set}(\mathbf{b})$,

2. **a** *has no repetitions.*

Furthermore,

3. $n \le m$*,*

4. $n = m$ *if and only if* **b** *has no repetitions, in which case* $\mathbf{a} = \mathbf{b}$*.*

Proof of Lemma 7. If **b** has no repetitions, then we take **a** to be **b**, and we are done.

Now suppose that **b** has at least one repetition.

We are going to show how to remove one repetition. And after we do that we will discuss how to remove all the repetitions.

Removal of one repetition: Since we are assuming that **b** has at least one repetition, we can pick two indices $i_1, i_2 \in \mathbb{N}_m$ such that $i_1 < i_2$ and $b_{i_1} = b_{i_2}$.

We then remove the entry b_{i_2}, taking care of moving b_{i_2+1} to the i_2-th place, b_{i_2+2} to the $i_2 + 1$-th place, and so on.

(So, for example, if we want to remove the entry b_8, we take $b_j^{(1)} = b_j$ for $j = 1, 2, 3, 4, 5, 6, 7$, but then we let $b_8^{(1)} = b_9$, $b_9^{(1)} = b_{10}$, and so on.)

Precisely, we define a new list $\mathbf{b^{(1)}} = (b_j^{(1)})_{j=1}^{m-1}$ by letting

$$b_j^{(1)} = \begin{cases} b_j & \text{if} \quad j < i_2 \\ b_{j+1} & \text{if} \quad j \ge i_2 \end{cases} .$$

The new list $\mathbf{b^{(1)}}$ has one fewer entry than **b**, and has exactly the same set of entries as **b** (that is, $\mathrm{Set}(\mathbf{b^{(1)}}) = \mathrm{Set}(\mathbf{b})$), because the entry of **b** that has been removed also occurs elsewhere in **b**, so the set of entries does not change.

If $\mathbf{b^{(1)}}$ has no repetitions, then we take $\mathbf{a} = \mathbf{b^{(1)}}$, and we are done.

Removal of all the repetitions: If $\mathbf{b^{(1)}}$ has a repetition, then we repeat the repetition removal process, and form a list $\mathbf{b^{(2)}}$.

And we continue in this way, removing one repetition at a time, until the process stops,

The process will stop when we get to a list $\mathbf{b^{(r)}}$ that has no repetitions. And when we get there, we can take **a** to be $\mathbf{b^{(r)}}$, and we are done. **Q**.**E**.**D**.[Lemma 7]

Remark 35. Exactly how do we know that this process will stop?

This was discussed in Remark 31, where we analyzed another entry removal process. The reasons that the process has to stop are the same:

- Intuitively, the process has to stop because at every step the length of the list goes down by 1, and the length can never be negative.
- A more rigorous way to say this is to invoke the well-ordering principle as follows: let S be the set of all the lengths of all the lists produced by this process. Then S is a set of nonnegative integers. By the well-ordering principle, S has a smallest member s. Then s is a nonnegative integer. and the process must stop at step s. □

21.2.1 Can we talk about the cardinality of a finite set?

So far, in Definition 66, we have introduced and defined the two-variable predicate "S has n members". Let us call this predicate $M(S,n)$, so "$M(S,n)$" stands for "S has n members".

We would like to say, when $M(S,n)$ holds, that "n is ***the*** cardinality (or ***the*** number of members) of S".

But in order to do that, we have to know that n is unique, that is, that if $M(S,n)$ holds, and m is a nonnegative integer such that $M(S,m)$ also holds, then m has to be equal to n.

This may seem obvious to you, but it still needs a proof.

Theorem 74. *Let p,q be nonnegative integers, and let S be a set such that S has p members and S has q members in the sense of Definition 66. Then $p=q$.*

Theorem 74 says that ***if there exists a nonnegative integer n such that S has n members, then n is unique.***

In order to prove the theorem, we will a lemma, which probably deserves the name "the stupidest lemma ever". It says that ***if you have a set S with n members and you remove one member s from S, then you get a set with $n-1$ members.*** Nothing could be more evident than that, right? Sure, but if it is evident, then it should be possible to prove it. So let us state it precisely and then prove it. (And the proof is going to be the obvious argument: make a list **a** without repetitions of all the members of S, remove s from the list, and you get a list **b** without repetitions of all the members of $S-\{s\}$. And ***that's all***.)

Lemma 8. *If S is a set and n is a nonnegative integer such that S has n members according to Definition 66, then*

1. *$S = \emptyset$ if and only if $n = 0$,*
2. *If $S \neq \emptyset$, and s is a member of S, then the set $S - \{s\}$ has $n - 1$ members.*

Proof of the lemma. Since S has n members, Definition 66 says that either $S = \emptyset \wedge n = 0$ or $S \neq \emptyset \wedge n \neq 0$. And in both cases the biconditional sentence "$S = \emptyset \Longleftrightarrow n = 0$" is true. (Remember that a biconditional $P \Longleftrightarrow Q$ is true if either P and Q are both true or P and Q are both false!) This proves Part 1.

To prove Part 2, suppose $S \neq \emptyset$, and $s \in S$. Since S has n members, Definition 66 tells us that we may pick a finite list $\mathbf{a} = (a_j)_{j=1}^{n}$ without repetitions such that $\mathbf{a}$ is a list of all the members of S.

Since $s \in S$, and $\mathbf{a}$ is a list of all the members of S, s must be one of the entries of $\mathbf{a}$. That is, we can pick an index $i \in \mathbb{N}_n$ such that $a_i = s$.

Our goal is to prove that $S - \{s\}$ has $n - 1$ members, and for that purpose we need to produce a finite list $\mathbf{b} = (b_j)_{j=1}^{n-1}$ of length $n - 1$ which is a list without repetitions of all the members of $S - \{s\}$.

In order to construct such a list, we do the most obvious thing: we remove s from $\mathbf{a}$. Precisely, we define a list $\mathbf{b} = (b_j)_{j=1}^{n-1}$ by letting

$$b_j = \begin{cases} a_j & \text{if} \quad j \in \mathbb{N},\ j < i \\ a_{j+1} & \text{if} \quad j \in \mathbb{N},\ i \leq j < n \end{cases} .$$

(For example, if we start with a list $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5, a_6)$, and $s = a_4$, then $\mathbf{b} = (a_1, a_2, a_3, a_5, a_6)$, so that $b_1 = a_1$, $b_2 = a_2$, $b_3 = a_3$, $b_4 = a_5$, and $b_5 = a_6$.)

Then $\mathbf{b}$ is a finite list of length $n - 1$. Furthermore, $\mathbf{b}$ is a list without repetitions. (This is very easy to prove. **YOU DO IT.**)

And, finally, $\mathbf{b}$ is a list of all the members of $S - \{s\}$. (This is also very easy to prove. **YOU DO IT.**)

So we have found a finite list of length $n - 1$ which is a list without repetitions of all the members of $S - \{s\}$.

This proves, according to Definition 66, that $S - \{s\}$ has $n - 1$ members. **Q.E.D.**[Lemma 8]

Proof of Theorem 74. As before, we write "$M(S, n)$" for "S has n members". We want to prove that

$$(\forall p \in \mathbb{N})(\forall q \in \mathbb{N})(\forall S)\Big((M(S,p) \wedge M(S,q)) \Longrightarrow p = q\Big) . \tag{21.7}$$

We rewrite the above proposition as

$$(\forall p \in \mathbb{N})A(p)\,,$$

where $A(p)$ is the sentence

$$(\forall q \in \mathbb{N})(\forall S)\Big((M(S,p) \wedge M(S,q)) \Longrightarrow p = q\Big)\,.$$

So our goal is to prove $(\forall p \in \mathbb{N})A(p)$. And we will do that by induction.

Base step. $A(0)$ says "if S has zero members and S has q members then $q = 0$."And this is true because it follows from Lemma 8 that $M(S,0)$ implies $S = \emptyset$, and $M(\emptyset, q)$ implies $q = 0$.

Inductive step. We have to prove that $(\forall p \in \mathbb{N})(A(p) \Longrightarrow A(p+1))$.

Let $p \in \mathbb{N} \cup \{0\}$ be arbitrary.

We want to prove that $A(p) \Longrightarrow A(p+1)$.

Assume that $A(p)$ holds. We want to prove $A(p+1)$.
That is, we want to prove that
$(\forall q \in \mathbb{N})(\forall S)\Big((M(S,p+1) \wedge M(S,q)) \Longrightarrow p+1 = q\Big)\,.$

Let $q \in \mathbb{N} \cup \{0\}$ be arbitrary and let S be an arbitrary set.
Assume that $M(S,p+1)$ and $M(S,q)$ hold, that is, S has $p+1$ members and S has q members.
Pick a member s of S, and let $S' = S - \{s\}$.
Then by Lemma 8 S' has p members and also $q-1$ members.

That is, $M(S',p) \wedge M(S',q-1)$.
But $(M(S',p) \wedge M(S',q-1)) \Longrightarrow p = q-1$, because we are assuming that $A(p)$ holds,
Since we know that $M(S',p) \wedge M(S',q-1)$, we can conclude (using Rule $\Longrightarrow_{use}$, i.e., the *Modus Ponens* rule) that $p = q-1$.

Then $p+1 = q$.

We have proved that $p+1 = q$ assuming that $M(S,p+1)$ and $M(S,q)$ hold. So we have proved (thanks to Rule $\Longrightarrow_{prove}$) that

$$(M(S,p+1) \wedge M(S,q)) \Longrightarrow p+1 = q\,. \tag{21.8}$$

And (21.8) was proved for arbitrary $q \in \mathbb{N} \cup \{0\}$ and an arbitrary set S. So we have proved (thanks to Rule $\forall_{prove}$)

$$(\forall q \in \mathbb{N})(\forall S)\Big((M(S,p+1) \wedge M(S,q)) \Longrightarrow p+1=q\Big)\,. \quad (21.9)$$

That is, we have proved $A(p+1)$.

Since we proved $A(p+1)$ assuming $A(p)$, we have proved (thanks to Rule $\Longrightarrow_{prove}$) that $A(p) \Longrightarrow A(p+1)$.

And, since we have proved that $A(p) \Longrightarrow A(p+1)$ for arbitrary $p \in \mathbb{N} \cup \{0\}$, we have proved (thanks to Rule $\forall_{prove}$) that $(\forall p \in \mathbb{N})(A(p) \Longrightarrow A(p+1))$. This completes the inductive step.

The PMI then implies that $(\forall p \in \mathbb{N})A(p)$, which is what we wanted to prove. **Q**.**E**.**D**.(Theorem 74)

Problem 50. ***Give a detailed proof*** of the two statements marked "YOU DO IT" in the proof of Lemma 8. □

And now, finally we can talk about ***the*** number of members of a finite set S, and give it a name.

The cardinality of a finite set

If S is a finite set then Fact 3 tells us that S has n members for some $n \in \mathbb{N} \cup \{0\}$, and Theorem 74 says that this n is unique.
So we can talk about ***the*** number of members of a finite set S. And we will also call this number the ***cardinality*** of S, and use the expression $\text{card}(S)$ to denote it.

Definition 67. Let S be a finite set. Then the cardinality of S is the nonnegative integer $\text{card}(S)$ defined as follows: $\text{card}(S)$ is the unique nonnegative integer n such that S has n members (i.e., S has cardinality n. □

21.3 Counting

In this section we discuss several "counting" problems of the following general form: *suppose that a set A is related in some way to some set B (or to two sets B_1, B_2, or to several sets $B_1, B_2, \ldots, B_n$). If the sets B_j are finite, can we conclude that A is finite? And can we determine the cardinality of A, or at least say something nontrivial about* $\text{card}(A)$*?*

In all the problems we will discuss, the conclusion will be of the form "A is finite and ...". But we will often omit the statement "A is finite", on the grounds that, if we prove that $\text{card}(A) = n$ for some nonnegative integer n, then it follows automatically that A is finite, so we don't need to say that separately.

We will look at:

1. Subsets of a finite set.

2. The union of two or more finite sets.

3. The power set of a finite set.

4. The Cartesian product of two finite sets.

5. Sets of lists of members of a set.

6. Sets of subsets of a set.

And, in order to be able to do that, we will prove in subsection 21.3.5 a general "counting principle" that will help us find cardinalities of lots of finite sets.

21.3.1 The cardinality of a subset of a finite set

Theorem 75. *If A is a finite set and B is a subset of A, then*

1. *B is a finite set,*

2. $\text{card}(B) \leq \text{card}(A)$*,*

3. *if $B \neq A$ then* $\text{card}(B) < \text{card}(A)$*.*

Proof. We already proved, in Proposition 3, that B is finite.

Let $\mathbf{a} = (a_j)_{j=1}^n$ be a finite list without repetitions of all the members of A. Let $\mathbf{b} = (b_j)_{j=1}^m$ be a list obtained from $\mathbf{a}$ by removing all the entries that are not members of B.

Then $n = \text{card}(A)$ and $m = \text{card}(B)$. Since $\mathbf{b}$ was obtained form $\mathbf{a}$ by removing some entries, m is $\leq n$, And, if $B \neq A$, then there is at least one entry a_j of $\mathbf{a}$ that does not belong to B, so at least one entry is removed to go from $\mathbf{a}$ to $\mathbf{b}$, and then $m < n$. **Q.E.D.**

21.3.2 The cardinality of the union of two sets

In this subsection we look at the following question.

Question 12. *If A, B are finite sets, can we say something useful about the cardinality of the union $A \cup B$?* □

First a definition.

Definition 68. Two sets A, B are <u>disjoint</u> if $A \cap B = \emptyset$. □

And now we can prove the two main theorems about the cardinality of the union of two sets.

Theorem 76. *If A, B are disjoint finite sets, then $A \cup B$ is a finite set, and*

$$\mathrm{card}(A \cup B) = \mathrm{card}(A) + \mathrm{card}(B)\,. \tag{21.10}$$

Theorem 77. *If A, B are finite sets, then $A \cup B$ is a finite set, and*

$$\mathrm{card}(A \cup B) = \mathrm{card}(A) + \mathrm{card}(B) - \mathrm{card}(A \cap B) \tag{21.11}$$

Proof of Theorem 76. Let $\mathbf{a} = (a_j)_{j=1}^m$ be a finite list without repetitions of all the members of A, and let $\mathbf{b} = (b_j)_{j=1}^n$ be a finite list without repetitions of all the members of B.

Let $\mathbf{c}$ be the concatenation[5] $\mathbf{a}\#\mathbf{b}$ of the lists $\mathbf{a}$, $\mathbf{b}$.

Then it is easy to prove that

(*) $\mathbf{c}$ is a list without repetitions of all the members of $A \cup B$.

(**YOU SHOULD PROVE THIS.**)

It follows from (*) that $A \cup B$ is a finite set, and $\mathrm{card}(A \cup B) = m + n$. **Q.E.D.**[Theorem 76]

Proof of Theorem 77. Let $C = A - B$, that is,

$$C = \{x : x \in A \wedge x \notin B\}\,.$$

Let $D = B - A$, that is,

$$D = \{x : x \in B \wedge x \notin A\}\,.$$

Let $E = A \cap B$, that is,

$$E = \{x : x \in A \wedge x \in B\}\,.$$

Then C and E are subsets of A, and D is a subset of B, so C, D and E are finite sets.

[5] The concatenation of two lists was defined on page 393.

Also, $C \cup E = A$ and $C \cap E = \emptyset$. Therefore

$$\text{card}(A) = \text{card}(C) + \text{card}(E)\,.$$

Similarly, 000

$$\text{card}(B) = \text{card}(D) + \text{card}(E)\,.$$

Furthermore, $A \cup D = A \cup B$, and $A \cap D = \emptyset$.

Since A and D are disjoint finite sets, Theorem 76 implies that $A \cup B$ is a finite set, and

$$\text{card}(A \cup B) = \text{card}(A) + \text{card}(D)\,.$$

It follows from the above equations that

$$\begin{aligned}
\text{card}(A \cup B) + \text{card}(A \cap B) &= \text{card}(A \cup B) + \text{card}(E) \\
&= \Big(\text{card}(A) + \text{card}(D)\Big) + \text{card}(E) \\
&= \text{card}(A) + \Big(\text{card}(D) + \text{card}(E)\Big) \\
&= \text{card}(A) + \text{card}(B)\,,
\end{aligned}$$

so

$$\text{card}(A \cup B) + \text{card}(A \cap B) = \text{card}(A) + \text{card}(B)\,,$$

and then

$$\text{card}(A \cup B) = \text{card}(A) + \text{card}(B) - \text{card}(A \cap B)\,,$$

Q.E.D.[Theorem 77]

Example 67. In a group of 1000 people, there are 700 people who like coffee, and 650 people who like tea.

Can we say something about the number N of people who like both coffee and tea?

The answer is that with the information we have we cannot determine N exactly, but we can give a ***lower bound*** for N, that is, an integer B usch that we can guarantee that $N \geq B$.

Indeed, let A be the set of the people in our group who like coffee, and let B be the set of the people in our group who like tea.

Then we know that $\text{card}(A) = 700$ and $\text{card}(B) = 650$.

Also,

$$\text{card}(A \cup B) = \text{card}(A) + \text{card}(B) - \text{card}(A \cap B)\,,$$

so

$$\mathrm{card}(A \cap B) = \mathrm{card}(A) + \mathrm{card}(B) - \mathrm{card}(A \cup B)\,.$$

Since $\mathrm{card}(A) = 700$ and $\mathrm{card}(B) = 650$, we can conclude that

$$\mathrm{card}(A \cap B) = 1,350 - \mathrm{card}(A \cup B)\,,$$

But $\mathrm{card}(A \cup B) \leq 1,000$, so

$$-\mathrm{card}(A \cup B) \geq -1,000\,,$$

and then

$$1,350 - \mathrm{card}(A \cup B) \geq 1,350 - 1,000 = 350\,.$$

So

$$\mathrm{card}(A \cap B) \geq 350\,.$$

So we have proved that ***the number of people who like both coffee and tea is at least*** 350. □

21.3.3 The cardinality of the union of several pairwise disjoint sets

Now that we know something about the cardinality of the union $A \cup B$ of two finite sets, we can discuss the question:

Question 13. *If $\mathbf{A} = (A_j)_{j=1}^n$ is a finite list of finite sets, can we say something useful about the cardinality of the union of those sets?* □

First of all, we have to define the union $\bigcup_{k=1}^n A_k$ (or "$A_1 \cup A_2 \cup \cdots \cup A_n$") of the sets A_k.

And, as I am sure you will have guessed, it is going to be an inductive definition.

Definition 69. Let $\mathbf{A} = (A_j)_{j=1}^n$ be a finite list of sets. The <u>union</u> of $\mathbf{A}$ (or "the union of the A_j") is the set $\bigcup_{j=1}^n A_j$ (or "$A_1 \cup \cdots \cup A_n$") defined inductively as follows:

$$\begin{aligned} \bigcup_{j=1}^{1} A_j &= A_1\,, \\ \bigcup_{j=1}^{n+1} A_j &= \Big(\bigcup_{j=1}^{n} A_j\Big) \cup A_{n+1} \qquad \text{if} \quad n \in \mathbb{N}\,. \end{aligned}$$

Remark 36. In case you don't like inductive definitions, it is also possible to give a noninductive definition of $\bigcup_{j=1}^{n} A_j$. The following theorem tells us how to do it. □

Theorem 78. *Let* $\mathbf{A} = (A_j)_{j=1}^{n}$ *be a finite list of sets. Then*

$$\bigcup_{j=1}^{n} A_j = \{x : (\exists j \in \mathbb{N}_n) x \in A_j\} . \tag{21.12}$$

Proof. **YOU DO IT.**

Remark 37. Theorem 78 tells us that it is possible to give a noninductive definition of $\bigcup_{j=1}^{n} A_j$: instead of defining $\bigcup_{j=1}^{n} A_j$ as we did, we could have defined it to be the set $\{x : (\exists j \in \mathbb{N}_n) x \in A_j\}$. And then the theorem tells us that if we had done that we would have ended up with the same set. In other words: ***if we had defined*** $\bigcup_{j=1}^{n} A_j$ ***to be the set*** $\{x : (\exists j \in \mathbb{N}_n) x \in A_j\}$***, then this would have been an equivalent definition, in the sense that the result would have been exactly the same set.*** □

Problem 51. ***Prove*** Theorem 78. □

Now that we know what "$\bigcup_{j=1}^{n} A_j$" means, we would like to express the cardinality of $\bigcup_{j=1}^{n} A_j$ in terms of the cardinalities of the sets A_j. In the previous section we studied the case of two sets, and we saw that the nice formula $\text{card}(A \cup B) = \text{card}(A) + \text{card}(B)$ holds under the extra condition that A and B be disjoint.

So it is natural that for the case of more than two sets a similar condition will be needed. We will have to require that the sets be ***pairwise disjoint***, and we first have to define what that means.

Definition 70. Let $\mathbf{A} = (A_j)_{j=1}^{n}$ be a finite list of sets. We say that $\mathbf{A}$ is a pairwise disjoint list, or that the sets A_j are pairwise disjoint, if

$$A_i \cap A_j = \emptyset \qquad \text{whenever } i, j \in \mathbb{N}_n \text{ and } i \neq j .$$

And then we can state the result about the cardinality of a union of several pairwise disjoint sets:

Theorem 79. *Let $\mathbf{A} = (A_j)_{j=1}^n$ be a finite list of finite sets. Assume that the A_j are pairwise disjoint. Then*

$$\mathrm{card}\Big(\bigcup_{j=1}^n A_j\Big) = \sum_{j=1}^n \mathrm{card}(A_j)\,. \tag{21.13}$$

Proof. **YOU DO IT.**

Problem 52. ***Prove*** Theorem 79. Your proof should be by induction, and you will *have* to use the inductive definitions of "$\bigcup$" and "$\sum$", because those are the only things you know about "$\bigcup$" and "$\sum$", and you will have to use the definition of "pairwise disjoint". Also, you may need a lemma (for example, that if $\mathbf{A} = (A_j)_{j=1}^n$ is a finite list of sets, B is a set, and $A_j \cap B = \emptyset$ for every j, then $\Big(\bigcup_{j=1}^n A_j\Big) \cap B = \emptyset$). If you need such a lemma, ***prove*** it. □

21.3.4 The cardinality of the union of several finite sets: the inclusion-exclusion formula

In this section we discuss the following question:

Question 14. *If $\mathbf{A} = (A_j)_{j=1}^n$ is a finite list of finite sets, we know that the cardinality of the union of the sets is the sum of the cardinalities of the sets if the sets are pairwise disjoint. Can we say something useful about the cardinality of the union of the sets even if the sets are not pairwise disjoint.?* □

The answer is "yes, we can say something, but not much".

For two sets A_1, A_2, we saw in subsection 21.3.2 that

$$\mathrm{card}(A_1 \cup A_2) = \mathrm{card}(A_!) + \mathrm{card}(A_2) - \mathrm{card}(A_1 \cap A_2) \tag{21.14}$$

What about three sets? In this case, we get a formula like (21.14), but more complicated:

Theorem 80. *Let A_1, A_2, A_3 be finite sets. Then*

$$\begin{aligned}\mathrm{card}(A_1 \cup A_2 \cup A_3) \;&=\; \mathrm{card}(A_1) + \mathrm{card}(A_2) + \mathrm{card}(A_3) - \mathrm{card}(A_1 \cap A_2)\\ &-\mathrm{card}(A_1 \cap A_3) - \mathrm{card}(A_2 \cap A_3) + \mathrm{card}(A_1 \cap A_2 \cap A_3)\,. \end{aligned}\tag{21.15}$$

Proof.

$$\begin{aligned}
\mathrm{card}(A_1 \cup A_2 \cup A_3) &= \mathrm{card}\Big((A_1 \cup A_2) \cup A_3\Big) \\
&= \mathrm{card}(A_1 \cup A_2) + \mathrm{card}(A_3) - \mathrm{card}\Big((A_1 \cup A_2) \cap A_3\Big) \\
&= \mathrm{card}(A_1) + \mathrm{card}(A_2) - \mathrm{card}(A_1 \cap A_2) + \mathrm{card}(A_3) \\
&\quad -\mathrm{card}\Big((A_1 \cap A_3) \cup (A_2 \cap A_3)\Big) \\
&= \mathrm{card}(A_1) + \mathrm{card}(A_2) + \mathrm{card}(A_3) - \mathrm{card}(A_1 \cap A_2) \\
&\quad - \Bigg(\mathrm{card}(A_1 \cap A_3) + \mathrm{card}(A_2 \cap A_3) \\
&\quad -\mathrm{card}\Big((A_1 \cap A_3) \cap (A_2 \cap A_3)\Big)\Bigg) \\
&= \mathrm{card}(A_1) + \mathrm{card}(A_2) + \mathrm{card}(A_3) - \mathrm{card}(A_1 \cap A_2) \\
&\quad -\mathrm{card}(A_1 \cap A_3) - \mathrm{card}(A_2 \cap A_3) \\
&\quad +\mathrm{card}\Big((A_1 \cap A_2 \cap A_3)\,.
\end{aligned}$$

So

$$\begin{aligned}
\mathrm{card}(A_1 \cup A_2 \cup A_3) &= \mathrm{card}(A_1) + \mathrm{card}(A_2) + \mathrm{card}(A_3) \\
&\quad -\mathrm{card}(A_1 \cap A_2) - \mathrm{card}(A_1 \cap A_3) - \mathrm{card}(A_2 \cap A_3) \\
&\quad +\mathrm{card}(A_1 \cap A_2 \cap A_3)\,,
\end{aligned}$$

completing the proof. **Q.E.D.**

What can be said about the cardinality of a union $A_1 \cup A_2 \cup \cdots \cup A_n$ of several finite sets? The answer is the following result.

Theorem 81. (The inclusion-exclusion formula) *Let* $(A_1, A_2, \ldots, A_n)$ *be a finite list of finite sets. Then*

$$\mathrm{card}\Big(\bigcup_{j=1}^{n} A_j\Big) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} \mathrm{card}(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}) \quad (21.16)$$

Proof. **YOU DO IT.**

Problem 53.

1. ***Write out*** Formula (21.16) for $n = 2$ and $n = 3$, and ***verify*** that the results agrees with Formulas (21.11) and (21.15).

2. ***Prove*** Theorem 81. HINT: Do it by induction. The proof that I gave you of Theorem 80 is really the step $P(2) \Longrightarrow P(3)$. □

21.3.5 A general counting principle

In this section we present a general method for solving counting problems, that is, problems in which we want to find the number of members of a finite set.

We will consider the following general situation: we will assume we are given a way of "generating all the members of a set G in k steps", by making a sequence of k choices:

1. In step 1 we choose one of n_1 possibilities, by choosing an object o_1, which is a member of a set O_1 of "available options before step 1", such that O_1 has n_1 members.

2. In step 2, we choose one of n_2 possibilities, by choosing an object o_2, which is a member of a set O_2 of "available options after step 1 and before step 2", such that O_2 has n_2 members.

3. In step 3, we choose one of n_3 possibilities, by choosing an object o_3 which is a member of a set O_3 of "available options after step 2 and before step 3", such that O_3 has n_3 members.

....

k. In step k, we choose we choose one of n_k possibilities, by choosing an object o_k, a member of a set O_{k-1} of "available options after step $k-1$ and before step k", such that O_k has n_k members.

And we assume that to each "admissible sequence $\mathbf{o}$ of choices" (that is, each list $\mathbf{o} = (o_1, o_2, o_3, \ldots, o_k)$ such that $o_1 \in O_1$, $o_2 \in O_2$, and so on) we associate a member $g(\mathbf{o})$ of G, in such a way that every member of G arises in this way from one and only one sequence $\mathbf{o}$.

The result will then be that G has $n_1 \times n_2 \times n_3 \times \cdots \times n_k$ (that is, $\prod_{j=1}^{k} n_j$) members.

It is very important that ***the set of options available after step*** $j-1$ ***and before step*** j ***must be allowed to depend on all the choices made before step*** j. So the sets O_2, O_3, etc, should really be called $O_2(o_1)$, $O_3(o_1, o_2)$, $O_4(o_1, o_2, o_3)$, and so on, to indicate this dependence.

The following example should make this clear.

Solved problem 1. *Let G be the set of all lists $\mathbf{x} = (x_1, x_2, \ldots, x_{100})$ of 100 integers that have the following properties: $|x_1| \leq 3$, and $|x_{j+1} - x_j| \leq j$ for each $j \in \mathbb{N}_{99}$. How many members does G have?*

This is exactly a counting problem of the kind described above. We determine a list $\mathbf{x}$ in 100 steps, by making a choice at each step.

In step 1 we choose x_1, and we have 7 ways to do that, because the integer x_1 must satisfy the condition $|x_1| \leq 3$, so x_1 must belong to the 7-member set $O_1 = \{-3, -2, -1, 0, 1, 2, 3\}$.

Having chosen x_1 in step 1, we have to choose an integer x_2 in step 2 from the 3-member set $O_2(x_1) = \{x_1 - 1, x_1, x_1 + 1\}$ (because x_2 must satisfy $|x_2 - x_1| \leq 1$).

Having chosen x_2 in step 2, we have to choose x_3 in step 3 from the 5-member set $O_2(x_2) = \{x_2 - 2, x_2 - 1, x_2, x_2 + 1, x_2 + 2\}$ (because x_3 must satisfy $|x_3 - x_2| \leq 2$).

And so on. For each j, at step j we choose x_j from the set $O_j(x_1, \ldots, x_{j-1})$ given by

$$O_j(x_1, \ldots, x_{j-1}) = \{x \in \mathbb{Z} : |x - x_{j-1}| \leq j - 1\} ,$$

which has $2j - 1$ members.

So the numbers n_j are as follows: $n_1 = 7$, and $n_j = 2j-1$ for $2 \leq j \leq 100$.

And the counting principle will tell us that

$$\text{card}(G) = 7 \times \prod_{j=2}^{100} (2j - 1) .$$

Notice that ***the sets O_j are not fixed. They depend on the previous choices made. (In our case, O_j depends on x_{j-1}).*** □

And now we give a precise statement and proof of the counting principle.

We will assume that we are given the following data:

A. a natural number k (the "number of steps"),

B. a list $\mathbf{n} = (n_1, n_2, \ldots, n_k)$ of natural numbers, of length k, C1. a finite set O_1 (the "set of options available in Step 1") with n_1 members,

C2. for each $o_1 \in O_1$, a finite set $O_2(o_1)$, which may depend on o_1, but has n_2 members for every o_1,

C3. for each $o_1 \in O_1$, $o_2 \in O_2(o_1)$, a finite set $O_3(o_1, o_2)$, which may depend on o_1 and o_2, but has n_3 members for every o_1, o_2,

....

Cj. for each $o_1 \in O_1$, $o_2 \in O_2(o_1)$, …, $o_{j-1} \in O_{j-1}(o_1, o_2, \ldots, o_{j-2})$, a finite set $O_j(o_1, o_2, \ldots, o_{j-1})$, which may depend on all the previous o_i's (that is, on $o_1, o_2, \ldots, o_{j-1}$), but has n_j members for every $o_1, o_2, \ldots, o_{j-1}$,

....

Ck. for each $o_1 \in O_1$, $o_2 \in O_2(o_1)$, …, $o_{k-1} \in O_{k-1}(o_1, o_2, \ldots, o_{k-2})$, a finite set $O_k(o_1, o_2, \ldots, o_{k-1})$, which may depend on all the previous o_i's (that is, on $o_1, o_2, \ldots, o_{k-1}$), but has n_k members for every $o_1, o_2, \ldots, o_{k-1}$.

Using these data, we can introduce the notion of an ***admissible sequence of choices***. An admissible sequence of choices is a list $\mathbf{o} = (o_1, o_2, \ldots, o_k)$ such that

1. $o_1 \in O_1$,

2. $o_2 \in O_2(o_1)$,

3. $o_3 \in O_3(o_1, o_2)$,

....

j. $o_j \in O_j(o_1, o_2, o_3, \ldots, o_{j-1})$ for all $j \in \mathbb{N}$ such that $2 \leq j \leq k$,

....

k. $o_k \in O_k(o_1, o_2, o_3, \ldots, o_{k-1})$.

Suppose, furthermore, that

D. We are given a set G, and a way of associating to each admissible sequence $\mathbf{o}$ of choices a member $g(\mathbf{o})$ of G in such a way that every member of G is $g(\mathbf{o})$ for one and only one $\mathbf{o}$.

Under those circumstances, we have the following theorem:

Theorem 82. **(The counting principle)** *The set G described above has $n_1 \times n_2 \times \cdots \times n_k$ (that is, $\prod_{j=1}^{k} n_j$) members.*

Proof. We prove the result by induction on k.

The statement we are trying to prove is true for $k = 1$, because in that case the admissible lists of choices are just lists of length 1, whose single entry is a member of O_1. Since O_1 has n_1 members, there are exactly n_1 admissible lists of choices. If $\mathbf{a} = (a_1, a_2, \ldots, a_{n_1})$ is a list without repetitions of all these lists, then $(g(a_1), g(a_2), \ldots, g(a_k))$ is a list without repetitions of all the members of G.

Now let us assume that the statement we are trying to prove is true for a natural number k, and let us prove it for $k + 1$.

Assume we are given data as above, involving $k + 1$ steps.

Let Q_k be the set of all lists of admissible choices up to k steps, and let Q_{k+1} be the set of all lists of admissible choices up to $k + 1$ steps.

Then Q_k is the set of all lists $\mathbf{o} = (o_1, o_2, \ldots, o_k)$ such that $o_1 \in O_1$, $o_2 \in O_1(o_1)$, $o_3 \in O_2(o_1, o_2)$, …, $o_k \in O_k(o_1, o_2, \ldots, o_{k-1})$.

Then by the inductive assumption $P(k)$, the set Q_k has $\prod_{j=1}^{k} n_j$ members. This means, if we let $\nu = \prod_{j=1}^{k} n_j$, that there are ν lists belonging to Q_k.

Now, all the members of the set Q_{k+1} can be obtained by taking a list $\mathbf{o} = (o_1, o_2, \ldots, o_k)$ belonging to Q_k and adding one more entry o_{k+1} to $\mathbf{o}$, where o_{k+1} is any member of the set $O_{k+1}(o_1, o_2, \ldots, o_k)$. This means that every list $\mathbf{o} \in Q_k$ gives rise to n_{k+1} lists in Q_{k+1}. It follows from this that Q_{k+1} has $n_{k+1}\nu$ members. That is, the cardinality of Q_{k+1} is $\prod_{j=1}^{k+1} n_j$.

On the other hand, the members of the set G are obtained from the members of Q_{k+1} as follows:

1. Each $\mathbf{o} \in Q_{k+1}$ gives rise to a member $g(\mathbf{o})$ of G.

2. Each member x of G is equal to $g(\mathbf{o})$ for one and only one $\mathbf{o} \in Q_{k+1}$.

Now let $\mu = \prod_{j=1}^{k+1} n_j$. Let $\mathbf{q} = (q_1, q_2, \ldots, q_\mu)$ be a list without repetitions of all the members of Q_{k+1}. Then $\mathbf{p} = (g(q_1), g(q_2), \ldots, g(q_\mu))$ is a list without repetitions of all the members of G. (It's a list of members of G because for every j $g(q_j)$ is a member of G, since q_j is in Q_{k+1}. It's a list of all the members of G because every $x \in G$ is equal to $g(q)$ for some $q \in Q_{k+1}$, and then $q = q_j$ for some j, because $\mathbf{q}$ is a list of all the members of Q_{k+1}. Finally, $\mathbf{p}$ is a list without repetitions because, if there was a repetition in $\mathbf{p}$, that is, a pair of indices $i, j \in \mathbb{N}_\mu$ such that $i \neq j$ but $g(q_i) = g(q_j)$, it would follow that $q_i = q_j$, because every member x of G is $g(q)$ for a unique $q \in Q_{k+1}$, so if we let $x = g(q_i)$, then $x = g(q_j)$ as well, and the uniqueness of q says that $q_i = q_j$, contradicting the fact that $\mathbf{q}$ is a list without repetitions.

So $\text{card}(G) = \mu$, and this completes the proof of $P(k+1)$, assuming $P(k)$, for an arbitrary $k \in \mathbb{N}$. This completes the proof of the theorem. **Q.E.D.**

21.3.6 The cardinality of a power set

In this section we discuss the following question:

Question 15. *If A is a finite set, what is the cardinality of the power set $\mathcal{P}(A)$ of A? In other words:* ***if A is a finite set, how many subsets does A have?*** □

The answer to this question turns out to be quite simple and precise: ***if A has n members then the power set $\mathcal{P}(A)$ has 2^n members***. That is:

Theorem 83. *If A is a finite set, then the power set $\mathcal{P}(A)$ is a finite set, and*

$$\text{card}\Big(\mathcal{P}(A)\Big) = 2^{\text{card}(A)}\,. \tag{21.17}$$

Proof. Let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ be a list without repetitions of all the members of A.

We can generate an arbitrary member X of $\mathcal{P}(A)$ in n steps, as follows:

In step 1, we decide whether or not a_1 is going to be in X. This can be done in two ways.

In step 2, we decide whether or not a_2 is going to be in X. This can be done in two ways.

. . . .

In step n, we decide whether or not a_n is going to be in X. This can be done in two ways.

So we generate all the members of $\mathcal{P}(A)$ in n steps, with two choices at each step. So the total number if subsets of A is the product of n factors, each one equal to 2, that is, 2^n. **Q.E.D.**

Problem 54. If A is a finite set, we define

$$\begin{aligned}\mathcal{P}_{even}(A) &= \Big\{X \in \mathcal{P}(A) : \text{card}(X) \text{ is even}\Big\}\\ \mathcal{P}_{odd}(A) &= \Big\{X \in \mathcal{P}(A) : \text{card}(X) \text{ is odd}\Big\}.\end{aligned}$$

So $\mathcal{P}_{even}(A)$ is the set of all subsets of A that have an even number of members, and $\mathcal{P}_{odd}(A)$ is the set of all subsets of A that have an odd number of members.

1. ***Prove*** that if A is a nonempty finite set, then

   $$\text{card}\Big(\mathcal{P}_{even}(A)\Big) = \text{card}\Big(\mathcal{P}_{odd}(A)\Big).$$

   (That is, if you call a subset of A "even" if has an even number of members and "odd" if has an odd number of members then you have to prove that A has as many even subsets as odd subsets. And, naturally, this will imply that, if $n = \text{card}(A)$, that each of the sets $\mathcal{P}_{even}(A)$, $\mathcal{P}_{odd}(A)$ has 2^{n-1} members.)

2. ***Explain*** why the assumption that A is nonempty is necessary, by describing what happens if $A = \emptyset$.

3. ***Verify*** the statement proved in Part 1, by listing all the subsets of the following sets, and counting how many have an even cardinality and how many have an odd cardinality:

   $$\begin{aligned}&\{\alpha, \beta, \gamma\}\\ &\{u, v, w, x\},\end{aligned}$$

   where α, β, γ are three different objects and u, v, w, x are four different objects.

HINT: There is a very easy way to do this problem if $\text{card}(A)$ is odd. In this case, you can prove the result as follows: using X^c to denote the complement of X relative to A (that is, writing "X^c" for "$A - X$"), then: (i) if X is even then X^c is odd, and (ii) if X is odd then X^c is even. So, if $\mathbf{X} = (X_j)_{j=1}^m$ is a list without repetitions of all the members of $\mathcal{P}_{even}(A)$, it follows that $\mathbf{Y} = (X_j^c)_{j=1}^m$ is a list without repetitions of all the members of $\mathcal{P}_{odd}(A)$. So $\text{card}\Big(\mathcal{P}_{even}(A)\Big) = \text{card}\Big(\mathcal{P}_{odd}(A)\Big)$.

Unfortunately, ***this method does not work if*** card(A) ***is even***, because in that case if X is even then X^c is also even, and if X is odd then X^c is also odd, so you cannot match the two sets $\mathcal{P}_{even}(A)$, $\mathcal{P}_{odd}(A)$ by pairing each member X of $\mathcal{P}_{even}(A)$ with its complement X^c.

So you need a more sophisticated argument. I suggest you use the counting principle. In order to generate all the members of $\mathcal{P}_{even}(A)$, do the same n-step counting as in the proof of Theorem 83, but observe that you can stop after step $n-1$ because, once you have decided for each of the first $n-1$ a_j's whether it is going to be in X or not, you are no longer free to make a decision about a_n: since the set X you are trying to create has to have an even number of members, then, if you already have an even number of members of X before step n, you have no choice but to leave a_n out, whereas if you have an odd number of members, then you have to put a_n in. □

21.3.7 The cardinality of a Cartesian product

In this section we discuss the following question:

Question 16. *If A, B are finite sets, what is the cardinality of the Cartesian product $A \times B$? In other words:* ***if A, B are finite sets, how many subsets does $A \times B$ have?*** □

First we recall the definition of ***Cartesian product***:

Definition 71. IF A, B are sets, the Cartesian product of A and B is the set $A \times B$ whose members are all the ordered pairs (a, b) consisting of a member a of A and a member n of B. That is,

$$A \times B = \{\, u : (\exists a \in A)(\exists b \in B) u = (a, b) \,\}\,.$$

or

$$A \times B = \{\, (a, b) : a \in A \wedge b \in B \,\}\,.$$

The answer to Question 16 is given by the following theorem:

Theorem 84. *Let A, B be finite sets. Then the Cartesian product $A \times B$ is finite set, and*

$$\mathrm{card}(A \times B) = \mathrm{card}(A) \times \mathrm{card}(B)\,. \tag{21.18}$$

Proof. Let $m = \mathrm{card}(A)$, $n = \mathrm{card}(B)$.

We can generate all the members (a, b) of $A \times B$ in two steps:

Step 1: Choose a. This can be done in m ways.

Step 2: Choose b. This can be done in n ways.

So the total number of ways in which we can generate an arbitrary member of $A \times B$ is mn.

This prove (21.18). **Q.E.D.**

21.3.8 Sets of lists

In this section we discuss the following question:

Question 17. *If A is a finite set of cardinality n, and k is a nonnegative integer, how many lists of members of A of length k are there? And we are interested in the following two kinds of lists:*

1. *Lists allowed to have repetitions.*
2. *Lists without repetitions.*

Let us rephrase our question in more formal language.

For a set A, and a nonnegative integer k, we define two sets, $\mathrm{List}_k(A)$ and $\mathrm{List}_k^{norep}(A)$, as follows:

1. $\mathrm{List}_k(A)$ is the set of all lists $\mathbf{a} = (a_j)_{j=1}^k$ of members of A of length k.
2. $\mathrm{List}_k^{norep}(A)$ is the set of all lists $\mathbf{a} = (a_j)_{j=1}^k$ without repetition of members of A of length k.

That is,

$$\begin{aligned}\mathrm{List}_k(A) &= \{\mathbf{a} = (a_j)_{j=1}^k : (\forall j \in \mathbb{N}_k) a_j \in A\}\,,\\ \mathrm{List}_k^{norep}(A) &= \{\mathbf{a} = (a_j)_{j=1}^k : \mathbf{a} \in \mathrm{List}_k(A) \wedge (\forall i, j \in \mathbb{N}_k)(i \neq j \Longrightarrow a_i \neq a_j)\}.\end{aligned}$$

We want to prove that the sets $\mathrm{List}_k(A)$ and $\mathrm{List}_k^{norep}(A)$ are finite, and determine their cardinalities.

Counting all lists of length k, possibly with repetitions, is easy.

Theorem 85. *Let A be a finite set, let $n = \mathrm{card}(A)$, and let k be a nonnegative integer. Then the set* $\mathrm{List}_k(A)$ *is finite, and*

$$\mathrm{card}\Big(\mathrm{List}_k(A)\Big) = n^k\,. \tag{21.19}$$

Proof. We can generate all the members $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ of $\mathrm{List}_k(A)$ in k steps:

Step 1: Choose a_1. This can be done in n ways.

Step 2: Choose a_2. This can be done in n ways.

....

Step k: Choose a_k. This can be done in n ways.

So the total number of ways in which we can generate an arbitrary member of $\mathrm{List}_k(A)$ is n^k.

This proves (21.19). **Q.E.D.**

We now count all lists of length k without with repetitions. This is also rather easy.

Theorem 86. *Let A be a finite set, let $n = \mathrm{card}(A)$, and let k be a nonnegative integer. Then the set* $\mathrm{List}_k^{norep}(A)$ *is finite, and*

$$\mathrm{card}\Big(\mathrm{List}_k^{norep}(A)\Big) = \left\{ \begin{array}{ccc} \frac{n!}{(n-k)!} & \text{if} & k \le n \\ 0 & \text{if} & k > n \end{array} \right. . \tag{21.20}$$

Proof. If $k > n$, then the set $\mathrm{List}_k^{norep}(A)$ is clearly empty, so

$$\mathrm{card}\Big(\mathrm{List}_k^{norep}(A)\Big) = 0\,,$$

in agreement with (21.20).

Now let us consider the case when $k \le n$.

In this case, we can generate all the members $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ of $\mathrm{List}_k^{norep}(A)$ in k steps:

Step 1: Choose a_1. This can be done in n ways.

Step 2: Choose a_2. This can be done in $n - 1$ ways, because after we have chosen a_1 in step 1 we are no longer allowed to choose a_2 to be equal to a_1, so there are only $n - 1$ possible values for a_2.

Step 3: Choose a_3. This can be done in $n-2$ ways, because after we have chosen a_1 and a_2 in steps 1, 2 we are no longer allowed to choose a_3 to be equal to a_1 or to a_2, so there are only $n-2$ possible values for a_3.

. . . .

Step k: Choose a_k. This can be done in $n-(k-1)$ ways, because after we have chosen $a_1, a_2, \ldots, a_{k-1}$ in steps $1, 2, \ldots, k-1$ we are no longer allowed to choose a_k to be equal to any of the a_j for $j = 1, 2, \ldots, k-1$, so there are only $n-(k-1)$ possible values for a_k.

So the number of members of $\mathrm{List}_k^{norep}(A)$ is the product $\prod_{j=1}^k q_j$ of k factors $q_1, q_2, \ldots, q_k$, where $q_1 = n$, $q_2 = n-1$, $q_3 = n-2$, and so on, until we get to $q_k = n-(k-1)$. Then $q_j = n-(j-1)$ for $j = 1, 2, \ldots, k$. That is,

$$\mathrm{card}\Big(\mathrm{List}_k^{norep}(A)\Big) = \prod_{j=1}^{k}(n-(j-1))\,,$$

or

$$\mathrm{card}\Big(\mathrm{List}_k^{norep}(A)\Big) = n \times (n-1) \times \cdots \times (n-(k-1))\,.$$

Since

$$\begin{aligned}\prod_{j=1}^{k}(n-(j-1)) &= \frac{\prod_{j=1}^{n}(n-(j-1))}{\prod_{j=k+1}^{n}(n-(j-1))}\\ &= \frac{\prod_{i=1}^{n} i}{\prod_{i=1}^{n-k} i}\\ &= \frac{n!}{(n-k)!}\end{aligned}$$

(where we have made the change of variables $i = n-(j-1)$, and used the facts that (i) as j varies from 1 to n, i varies from n to 1, and (ii) as j varies from $k+1$ to n, i varies from $n-k$ to 1), it follows that

$$\mathrm{card}\Big(\mathrm{List}_k^{norep}(A)\Big) == \frac{n!}{(n-k)!}\,.$$

So our result is proved. **Q.E.D.**

21.3.9 Enumerations and permutations

Definition 72. If A is a finite set, a list without repetitions of all the members of A is called an enumeration of A, or a permutation of A. □

It is clear that the set of all enumerations of A is the set $\mathrm{List}^{norep}_{\mathrm{card}(A)}(A)$ of all lists of length card(A) of members of A without repetitions. So we get

Theorem 87. *The number of enumerations of a finite set A with cardinality n is $n!$.*

Proof. Theorem 86 says that if $\mathrm{card}(A) = n$, $k \in \mathbb{N} \cup \{0\}$, and $k \geq n$, then $\mathrm{card}\Big(\mathrm{List}^{norep}_k(A)\Big) = \frac{n!}{(n-k)!}$. In our case, $k = n$, so $n - k = 0$, and $(n-k)! = 1$ (because $0! = 1$), so we get $\mathrm{card}(\mathrm{List}^{norep}_n(A)) = n!$. **Q.E.D.**

21.3.10 The binomial coefficients

We recall the definition of the ***binomial coefficients***, given earlier:

Definition 73. If n, k are nonnegative integers such that $k \leq n$, then the binomial coefficient $\left(\begin{array}{c} n \\ k \end{array}\right)$ is defined by the formula

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \,. \tag{21.21}$$

One of the most important facts about the numbers $\left(\begin{array}{c} n \\ k \end{array}\right)$ is that ***they are always integers***.

Remark 38. It is not obvious at all from the definition that $\binom{n}{k}$ is always an integer.

For example: ***why should*** $\binom{17}{9}$ ***be an integer? Why does*** $17!$ ***have to be divisible by*** $9! \times 8!$***?*** There is no doubt that $17!$ has to be divisible by $9!$, because $17! = 17 \times 16 \times 15 \times 14 \times 13 \times 12 \times 11 \times 10 \times 9!$. But why is the quotient

$$\frac{17!}{9!} = 17 \times 16 \times 15 \times 14 \times 13 \times 12 \times 11 \times 10$$

divisible by 8!? In this particular example, it is easy to do the cancellations, and get

$$\begin{aligned}\frac{17!}{8!9!} &= \frac{17\times 16\times 15\times 14\times 13\times 12\times 11\times 10}{8\times 7\times 6\times 5\times 4\times 3\times 2}\\ &= \frac{17\times 15\times 14\times 13\times 12\times 11\times 10}{7\times 6\times 5\times 4\times 3}\\ &= \frac{17\times 13\times 12\times 11\times 10}{6\times 2}\\ &= 17\times 13\times 11\times 10\end{aligned}$$

So in this particular case it is clear that $\left(\begin{array}{c}17\\9\end{array}\right)$ is an integer, but ***it is not clear yet why it should be true in general that*** $\left(\begin{array}{c}n\\k\end{array}\right)$ ***is an integer for all*** $n,k\in\mathbb{N}\cup\{0\}$ ***such that*** $k\le n$.

The following two theorems give one answer to this question. □

Theorem 88. *Let* $n,k\in\mathbb{N}\cup\{0\}$ *be such that* $1\le k\le n$. *Then*

$$\left(\begin{array}{c}n+1\\k\end{array}\right)=\left(\begin{array}{c}n\\k-1\end{array}\right)+\left(\begin{array}{c}n\\k\end{array}\right). \tag{21.22}$$

Proof. **YOU DO IT.**

Theorem 89. *If* n,k *are nonnegative integers such that* $k\le n$, *then the binomial coefficient* $\left(\begin{array}{c}n\\k\end{array}\right)$ *is an integer.*

Proof. **YOU DO IT.**

Problem 55. ***Prove*** Theorems 88 and 89.

The proof of Theorem 88 should be very easy: you just add the fractions $\frac{n!}{(k-1)!(n-(k-1))!}$ and $\frac{n!}{k!(n-k)!}$ and the answer turns out to be $\frac{(n+1)!}{k!(n-k)!}$.

The proof of Theorem 89 should be very easy, by induction. Theorem 88 easily implies that if all the binomial coefficients $\left(\begin{array}{c}n\\k\end{array}\right)$ are integers for a given n, then all the binomial coefficients $\left(\begin{array}{c}n+1\\k\end{array}\right)$ are integers as well. And this is basically the inductive step.

But ***you should write the proof carefully and correctly.*** In particular, pay attention to the fact that what you want to prove is a statement with ***two quantifiers***, but in a proof by induction of $(\forall n \in \mathbb{N} \cup \{0\})P(n)$, the sentence $P(n)$ has to have n as an open variable, and no other open variables. So you cannot take $P(n)$ to be a closed formula such as

$$(\forall n \in \mathbb{N} \cup \{0\})(\forall j \in \mathbb{N} \cup \{0\})\Big(k \leq n \Longrightarrow \begin{pmatrix} n \\ k \end{pmatrix} \in \mathbb{Z}\Big)\,,$$

and you cannot take $P(n)$ to be "$k \leq n \Longrightarrow \begin{pmatrix} n \\ k \end{pmatrix} \in \mathbb{Z}$" either, because this formula has two open variables.

Also, you should pay attention in your inductive step to the fact that Formula (21.22) cannot be applied if $k = 0$, so you will have to consider the case when $k = 0$ separately. □

21.3.11 Counting the number of subsets of a given cardinality

In this section we discuss the following question:

Question 18. *If A is a finite set of cardinality n, and k is a nonnegative integer, how many subsets with k members does A have?*

Let us rephrase our question in more formal language.

For a set A, and a nonnegative integer k, we define the set $\mathcal{P}_k(A)$ as follows: $\mathcal{P}_k(A)$ is the set of all subsets X of A such that $\mathrm{card}(X) = k$. That is,

$$\mathcal{P}_k(A) \quad = \quad \{\, X : X \subseteq A \wedge \mathrm{card}(X) = k \,\}\,.$$

Theorem 90. *Let A be a finite set, let $n = \mathrm{card}(A)$, and let k be a nonnegative integer. Then the set $\mathcal{P}_k(A)$ of all subsets of A that have k members is finite, and*

$$\mathrm{card}\Big(\mathcal{P}_k(A)\Big) = \begin{cases} \begin{pmatrix} n \\ k \end{pmatrix} & \text{if} \quad k \leq n \\ \quad 0 & \text{if} \quad k > n \end{cases}\,. \tag{21.23}$$

Proof. If $k > n$, then the set $\mathcal{P}_k(A)$ is clearly empty, so $\mathrm{card}\Big(\mathcal{P}_k(A)\Big) = 0$, in agreement with (21.23).

Now let us consider the case when $k \le n$.

In this case, instead of using our general counting principle to find the number $\mathrm{card}\Big(\mathcal{P}_k(A)\Big)$, we will use it to find a number that we already know, namely, $\mathrm{card}\Big(\mathrm{List}_k^{norep}(A)\Big)$.

The key idea is this: we will use a different way of generating the members of $\mathrm{List}_k^{norep}(A)$. And this will give as an equation for $\mathrm{card}\Big(\mathcal{P}_k(A)\Big)$ that we will be able to solve in order to find $\mathrm{card}\Big(\mathcal{P}_k(A)\Big)$.

We can generate all the members $\mathbf{a}$ of $\mathrm{List}_k^{norep}(A)$ (i.e., all the lists of length k of members of A without repetition) in two steps:

Step 1: Choose the set $\mathrm{Set}(\mathbf{a})$ of all the entries of $\mathbf{a}$. Since $\mathbf{a}$ has to be a list of length k without repetitions, the set S has to be a subset of A having k members. So *this step can be done in* $\mathrm{card}\Big(\mathcal{P}_k(A)\Big)$ *ways.*

Step 2: Having chosen the set S of entries, create the list $\mathbf{a}$. That is, create an enumeration of S. Since we already have the k entries of $\mathbf{a}$, there are $k!$ enumerations of S. (Reason: Theorem 87.)

Then the total number of members of $\mathrm{List}_k^{norep}(A)$ is $k! \times \mathrm{card}\Big(\mathcal{P}_k(A)\Big)$. That is,

$$\mathrm{card}\Big(\mathrm{List}_k^{norep}(A)\Big) = k! \times \mathrm{card}\Big(\mathcal{P}_k(A)\Big)\,.$$

But we already know that

$$\mathrm{card}\Big(\mathrm{List}_k^{norep}(A)\Big) = \frac{n!}{(n-k)!}\,,$$

It follows from the above formulas that

$$k! \times \mathrm{card}\Big(\mathcal{P}_k(A)\Big) = \frac{n!}{(n-k)!}\,,$$

Hence

$$\mathrm{card}\Big(\mathcal{P}_k(A)\Big) = \frac{n!}{k!(n-k)!}\,,$$

which is the desired result. **Q.E.D.**

21.3.12 Some simple counting problems, with some solutions

Solved problem 2. *In how many ways can the letters of the word MISSISSIPPI be rearranged?*

Solution. Let ν be the number of rearrangements that we are trying to determine.

We can create a rearrangement of the word MISSISSIPPI in three steps, as follows:

We first observe that a rearrangement of MISSISSIPPI will consist of putting one of the letters of MISSISSIPPI in each of 11 slots. Let us number the slots $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$. So the set of slots is $\mathbb{N}_{11}$, i.e., the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

And then, here are the three steps:

Step 1. We choose a subset U_1 with four members of the set $\mathbb{N}_{11}$. (These are the slots where we are going to put an S.) This can be done in n_1 ways, where n_1 is the number of 4-member subsets of a set with 11 members.

Step 2. We choose a subset U_2 with four members of the set $\mathbb{N}_{11} - U_1$. (These are the slots where we are going to put an I.) This can be done in n_2 ways, where n_2 is the number of 4-member subsets of a set with 7 members.)

Step 3. Now that we have three slots left, we have to put an M in one of them and two Ps in the remaining two slots. So all we have to do is choose the one slot where we will put the M. And this can be done in 3 ways.

So $\nu = 3n_1n_2$.

It follows from Theorem 90 that $n_1 = \binom{11}{4}$ and $n_2 = \binom{7}{4}$.

Hence $\nu = 3\binom{11}{4}\binom{7}{4}$.

Therefore

$$\begin{aligned}
\nu &= 3 \times \frac{11 \times 10 \times 9 \times 8}{4 \times 3 \times 3} \times \frac{7 \times 6 \times 5 \times 4}{4 \times 3 \times 2} \\
&= 3 \times 11 \times 10 \times 7 \times 3 \times 5 \\
&= 33 \times 70 \times 15 \\
&= 2,310 \times 15 \\
&= 34,650\,.
\end{aligned}$$

So *the number of rearrangements is equal to* 34,659. □

Problem 56. In how many ways is it posible to rearrange the letters of the word ABRACADABRA ? □

Solved problem 3. *In a group of* 100 *men and* 100 *women, in how many ways can the people be divided into* 100 *couples consisting of one man and one woman?*

Solution. First we make a list $\mathbf{w} = (w_j)_{j=1}^{100}$, without repetitions, of the 100 women.

Next we divide the people into couples in 100 steps, as follows:

Step 1. We choose a man m_1 to form a couple with w_1. This can be done in 100 ways.

Step 2. We choose a man m_2 to form a couple with w_2. This can be done in 99 ways, because m_1 is not available.

Step 3. We choose a man m_3 to form a couple with w_3. This can be done in 98 ways, because m_1 and m_2 are not available.

. . . .

Step 99. We choose a man m_{99} to form a couple with w_{99}. This can be done in 2 ways, because only two men are available, since at this point 98 men have already been chosen.

Step 100. We choose a man m_{100} to form a couple with w_{100}. This can be done in only one way, because only one man is still available, since at this point 99 men have already been chosen.

So *the total number of ways to form* 100 *couples is the product*

$$100 \times 99 \times 98 \times \cdots \times 2 \times 1\,,$$

that is, 100!. □

Solved problem 4. *If S is a finite set, how many unordered pairs $\{a, b\}$ such that $a \in S$, $b \in S$, and $a \neq b$ are there?*

Solution. The unordered pairs $\{a, b\}$ such that $a \in S$, $b \in S$, and $a \neq b$ are exactly the members of the set $\mathcal{P}_2(S)$ of all two-member subsets of S.

This number was computed in Theorem 90, where we found that

$$\text{card}\Big(\mathcal{P}_k(S)\Big) = \left(\begin{array}{c}\text{card}(S)\\ k\end{array}\right) \quad \text{whenever } \ k \in \mathbb{N}_n\,.$$

So

$$\mathrm{card}\Big(\mathcal{P}_2(S)\Big) = \left(\begin{array}{c}\mathrm{card}(S)\\ 2\end{array}\right) = \frac{1}{2}\mathrm{card}(S)(\mathrm{card}(S)-1)\,.$$

So *the number we have been asked to find is equal to* $\frac{1}{2}\mathrm{card}(S)(\mathrm{card}(S)-1)$. □

Solved problem 5. *In a group of* 200 *people, in how many ways can the people be divided into* 100 *sets consisting of two people each?*

Remark. The number we get for this problem should be much larger than the number we got for Problem 3. (Why? Divide the group of 200 people in any way you like, into two sets M, W of 100 members each, and label the members of M "men" and the members of W 'women". Then in Problem 3 we found out in how many ways one can form 100 couples consisting of one member of M and one member of W. But here we are asked to form 100 pairs in any way, not just man-woman pairs, so the number should be much larger.)

Solution. We solve this problem by solving another counting problem in two ways, and getting an equation for the number we want.

Let P be the given set of 200 people.

Let ν be the number we want to compute.

We compute the number $\alpha = \mathrm{card}\Big(\mathrm{List}_{200}^{norep}(P)\Big)$ of all lists without repetition of all the members of P, i.e., of all enumerations of P.

We already know from Theorem 87 that $\alpha = 200!$.

What we are going to do now is compute that very same number α in a different way, and this will give us an equation that we will be able to solve for ν.

We are going to describe a way to generate all the members of the set $\mathrm{List}_{200}^{norep}(P)$ in 102 steps. Here is how we can do that.

Step 1. We divide the set P into 100 sets with two members each, and we let Q be the set of 100 2-member subsets of P obtained in this way. Clearly, the number of ways to do this is ν.

Step 2. Now that we have a set Q of 100 unordered pairs $\{a,b\}$ of members of P, which are pairwise disjoint, we produce a list $\mathbf{q} = (q_j)_{j=1}^{100}$ without repetitions of all the members of Q (i.e., an enumeration of Q). Since Q has 100 members, this can be done in 100! ways.

Steps 3 to 102. Now that we have the list $\mathbf{q}$, in 100 steps we order each of the entries of $\mathbf{q}$. Remember that each entry q_j is an unordered pair $\{a, b\}$ consisting of two members of P. So we order this pair, that is, we choose one of the members of the set q_j and call it a_j, and call b_j the other member. In Step 3 we do this for q_1, in Step 4 we do this for q_2, and so on, until in Step 102 we do it for q_{100}.

Clearly, in each of the 100 steps we have two ways to order the pair q_j.

And now that are finished, we can easily produce a list $\mathbf{p}$ without repetitions of all the members of P: we let p_1 be a_1, p_2 be b_1, p_3 be a_2, p_4 be b_2, and so on. (In general, $p_{2j-1} = a_j$ and $p_{2j} = b_j$, for $j = 1, 2, \ldots, 100$.)

In this way we generate all the enumerations of P.

So there are $\nu \times 100! \times 2^{100}$ enumerations of P.

It follows that

$$\nu \times 100! \times 2^{100} = 200!\,.$$

Therefore

$$\nu = \frac{200!}{2^{100}100!}\,. \tag{21.24}$$

So, finally, we have shown that *the number of ways to divide a set with* 200 *members into* 100 2*-member sets is* $\frac{200!}{2^{100}100!}$. □

Problem 57. ***Prove*** that the number ν of equation (21.24) is equal to the product of all the odd natural numbers from 1 to 199. That is, prove that

$$\nu = \prod_{j=1}^{100}(2j-1)\,. \tag{21.25}$$

Problem 58. Since the number ν given by Equation (21.24) has such a simple expression, given by Equation (21.25), there *has* to be a reason for that. It has to be possible to find a simple way to generate the set $\mathcal{D}_{200,2}$ of all ways of dividing a set with 200 members into 100 2-member sets, in 100 steps, with $2j-1$ options in Step j, so that we can apply the counting principle and get Formula (21.25).

Find it. □

Problem 59. This problem deals with a generalization of Solved Problem 5.

Let m, q be natural numbers, and let $n = qm$.

In a set P of n people, in how many ways can the set P be divided into q sets each one of which has m members?.

NOTE: Solved Problem 5 was the case when $m = 2$, $q = 100$, $n = 200$. Here I am asking you to use the same idea as in our solution of Solved Problem 5 to do the more general case. □

Solved problem 6. A standard deck of playing cards contains 52 cards. There are 13 different ***ranks*** of cards, namely, $A, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q$ and K. And there are four ***suits***: Hearts, Spades, Diamonds and Clubs. For each rank r and each suit s, the standard 52-card deck contains exactly one card of rank r and suit s.

A poker hand is a set of five cards.

How many poker hands are there?

Solution. A poker hand is a 5-member subset of the 52-member set of all cards. According to Theorem the number of such subsets is $\begin{pmatrix} 52 \\ 5 \end{pmatrix}$.

So the solution of our problem is $\begin{pmatrix} 52 \\ 5 \end{pmatrix}$, which is equal to $\frac{52!}{5!\times 47!}$, i.e., to $\frac{52\times 51\times 50\times 49\times 48}{5\times 4\times 3\times 2}$. This fraction is in turn equal to $\mathbf{2,598,960}$.

So *the total number of poker hands is* $\mathbf{2,598,960}$*, which is about* $2,6$ *million.*

Solved problem 7. *This problem is a continuation of Solved Problem 6.*

If S is a set of hands, the probability of S is the real number $P(S)$ given by

$$P(S) = \frac{\text{card}(S)}{N}\,,$$

where N is the number of poker hands. (That is, $N = 2,598,960$.)

A poker hand is a full house if it consists of three cards of one rank and two cards of another rank.

How many full houses are there? And what is the probability of a full house?

Solution. We use the counting principle. We can generate all full house hands in four steps as follows:

Step 1, Choose which of the 13 ranks is going to be the one of which there are going to be three cards in the hand. This can be done in 13 ways.

Step 2, Choose which of the 12 ranks left after Step 1 is going to be the one of which there are going to be two cards in the hand. This can be done in 12 ways.

Step 3, Choose which three of the four cards of the rank chosen in step 1 are going to be the ones occurring in the hand. This can be done in 4 ways. (Choosing three out of four is the same as choosing one out of four, because choosing three out of four amounts to choosing the one card that will not be there. Mathematically, $\begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix} = 4$.)

Step 4, Choose which two of the four cards of the rank chosen in step 2 are going to be the ones occurring in the hand. This can be done in 6 ways, because $\begin{pmatrix} 4 \\ 2 \end{pmatrix} = 6$.

So the numbers n_1, n_2, n_3, n_4 are 13, 12, 4 and 6.

Hence the total number of full houses is 13 × 12 × 4 × 6, which is equal to $\mathbf{3,754}$.

So *the total number of full houses is* $\mathbf{3,754}$.

As for the probability of a fulls house, it is equal to the quotient $\frac{3{,}754}{2{,}598{,}960}$. This can be computed exactly, but to have an idea of its magnitude we just observe that $2,598,960$ is a little over $2,5$ million, so $\frac{3{,}754}{2{,}598{,}960}$ is a little under $\frac{3{,}754}{2{,}500{,}000}$, which equals $\frac{15{,}016}{10{,}000{,}000}$, that is, approximately, 15 in $10,000$, or 0.0015, or 0.15%.

So *the probability of a full house is approximately* 15 *in* $10,000$*, or* 0.0015*, or* 0.15 *percent.*

NOTE: A more accurate estimate can be obtained by observing that when we substituted $2,500,000$ for $2,598,960$ we made an error of about 1 in 25, that is 4%. This resulted in underestimating the denominator of the fraction $\frac{3{,}754}{2{,}598{,}960}$ by about 4%, so we overestimated the quotient by about 4%, So we must reduce the number we found by about 4%. And 4% of 0.15 is about 0.006. This means that a more accurate estimate of the probability is 0.144%.

NOTE: The exact value is 0.1441%. □

Problem 60. *This problem is a continuation of Solved Problems 6 and 7.*

A poker hand is a two pair hand if it consists of two cards of the same rank, two cards of another rank, and a fifth card of a rank different from the other two.

Determine the number of two pair hands, and the probability of a two pair hand. □

Problem 61. *This problem is a continuation of Solved Problems 6 and 7 and Problem 60 .*

A poker hand is a three of a kind hand if it consists of three cards of one rank and two cards of two different ranks.

Determine the number of three of a kind hands, and the probability of a three of a kind hand. □

21.4 The binomial theorem

You must have seen for sure the formula

$$(a+b)^2 = a^2 + 2ab + b^2\,, \tag{21.26}$$

and you probably have also seen the formula

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3\,, \tag{21.27}$$

and perhaps even the formula

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4\,. \tag{21.28}$$

You probably must have guessed from these three formulas that there is a general formula for $(a+b)^n$. What does this formula look like?

The formula that generalizes (21.26), (21.27), and (21.28), is the ***binomial formula***. And the statement that this formula is valid is the ***binomial theorem:***

The binomial theorem

Theorem 91. *If n is a natural number, and a, b are real numbers*[a]*, then*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\,. \tag{21.29}$$

[a] The formula is equally valid for members of any number system in which there are operations of addition and multiplication that obey the commutative laws, the associative laws, and the distributive law of multiplication with repsect to addition. So, for example, the formula is also valid for complex numbers, or for integers modulo N.

Proof of the binomial theorem. It will be more convenient to work first with objects that do not necessarily satisfy the commutative law of multiplication. (For example, a and b could be 2×2 matrices, or 3×3 matrices, or, more generally, $r \times r$ matrices for any $r \in \mathbb{N}$.) This will give us a formula whose structure will be be very clear. And then, by making the extra assumption that multiplication is commutative, we will see how the binomial coefficients arise.

The first few powers of $a + b$ are as follows:

$$\begin{aligned}
(a+b)^1 &= a+b \\
(a+b)^2 &= (a+b)(a+b) \\
&= (a+b)a + (a+b)b \\
&= aa + ba + ab + bb \\
(a+b)^3 &= (a+b)^2(a+b) \\
&= (aa+ba+ab+bb)(a+b) \\
&= (aa+ba+ab+bb)a + (aa+ba+ab+bb)b \\
&= aaa + baa + aba + bba + aab + bab + abb + bbb
\end{aligned}$$

$$\begin{aligned}
(a+b)^4 &= (a+b)^3(a+b)\\
&= (aaa+baa+aba+bba+aab+bab+abb+bbb)(a+b)\\
&= \quad (aaa+baa+aba+bba+aab+bab+abb+bbb)a\\
&\quad +(aaa+baa+aba+bba+aab+bab+abb+bbb)b\\
&= \quad aaaa+baaa+abaa+bbaa+aaba+baba+abba+bbba\\
&\quad +aaab+baab+abab+bbab+aabb+babb+abbb+bbbb\,.
\end{aligned}$$

It is clear that $(a+b)^3$ is the sum of 8 terms, each one of which is a product $q_1q_2q_3$ of three factors, where each factor q_j is either a or b. Furthermore, all possible such products occur in the sum.

And $(a+b)^4$ is the sum of 16 terms, each one of which is a product $q_1q_2q_3q_4$ of four factors, where each factor q_j is either a or b. And, again, all possible such products occur in the sum.

Let us make this precise, and prove that the same pattern occurs for every power $(a+b)^n$.

For each natural number n, let $Q_n(a,b)$ be the set of all lists $\mathbf{q}=(q_j)_{j=1}^n$ of length n such that each entry q_j is either a or b. (That is, $Q_n(a,b)$ is the set of all lists of length n of members of the set $\{a,b\}$.) Then it is clear that $Q_n(a,b)$ has 2^n members, (Reason: we can generate the lists $\mathbf{q}=(q_j)_{j=1}^n$ in n steps. In step 1 we choose q_1 to be either a or b. In step 2 we choose q_2 to be either a or b. And so on. There are two ways to make the choice in each step, so the total number of lists is 2^n.)

And, for each member $\mathbf{q}=(q_j)_{j=1}^n$ of $Q_n(a,b)$, let $\prod\mathbf{q}$ be the product $\prod_{j=1}^n q_j$.

Then we will prove:

Lemma 9. *The power $(a+b)^n$ is the sum of the products $\prod\mathbf{q}$ of all the lists $\mathbf{q}\in Q_n(a,b)$. That is,*

$$(a+b)^n=\sum_{\mathbf{q}\in Q_n(a,b)}\prod\mathbf{q}\,. \tag{21.30}$$

Proof of the lemma. Let $P(n)$ be the statement "$(a+b)^n=\sum_{\mathbf{q}\in Q_n(a,b)}\prod\mathbf{q}$". We prove $(\forall n\in\mathbb{N})P(n)$ by induction.

Base step. $P(1)$ says "$a+b=a+b$" (because $Q_1(a,b)$ consists of just two lists, namely, (a) and (b)). So $P(1)$ is true.

Inductive step. Let $n \in \mathbb{N}$ be arbitrary. Assume $P(n)$ is true. That means that

$$(a+b)^n = \sum_{\mathbf{q}\in Q_n(a,b)} \prod \mathbf{q}\,. \tag{21.31}$$

Then

$$\begin{aligned}(a+b)^{n+1} &= \Big(\sum_{\mathbf{q}\in Q_n(a,b)} \prod \mathbf{q}\Big)(a+b)\\ &= \Big(\sum_{\mathbf{q}\in Q_n(a,b)} \prod \mathbf{q}\Big)a + \Big(\sum_{\mathbf{q}\in Q_n(a,b)} \prod \mathbf{q}\Big)b\\ &= \Big(\sum_{\mathbf{q}\in Q_n(a,b)} (\prod \mathbf{q})a\Big) + \Big(\sum_{\mathbf{q}\in Q_n(a,b)} (\prod \mathbf{q})b\Big)\\ &= \Big(\sum_{\mathbf{q}\in Q_n(a,b)} \prod (\mathbf{q}\#(a))\Big) + \Big(\sum_{\mathbf{q}\in Q_n(a,b)} \prod \mathbf{q}\#(b)\Big)\,,\end{aligned}$$

where $\mathbf{q}\#(a)$, $\mathbf{q}\#(b)$, stand for the concatenations of the list $\mathbf{q}$ and the one-entry lists (a), (b) (that is, $\mathbf{q}\#(a) = (r_j)_{j=1}^{n+1}$, where $r_j = q_j$ for $j = 1,\ldots,n$, and $r_{n+1} = a$, and $\mathbf{q}\#(b) = (s_j)_{j=1}^{n+1}$, where $s_j = q_j$ for $j = 1,\ldots,n$, and $s_{n+1} = b$).

The 2^{n+1} lists $\mathbf{q}\#(a)$, $\mathbf{q}\#(b)$, as $\mathbf{q}$ ranges over all the lists $\mathbf{q} \in Q_n(a,b)$, are all the lists in $Q_{n+1}(a,b)$. Therefore

$$\Big(\sum_{\mathbf{q}\in Q_n(a,b)} \prod (\mathbf{q}\#(a))\Big) + \Big(\sum_{\mathbf{q}\in Q_n(a,b)} \prod \mathbf{q}\#(b)\Big) = \sum_{\mathbf{q}\in Q_{n+1}(a,b)} \prod \mathbf{q}\,,$$

and then

$$(a+b)^{n+1} = \sum_{\mathbf{q}\in Q_{n+1}(a,b)} \prod \mathbf{q}\,. \tag{21.32}$$

So $P(n+1)$ holds.

Then the PMI implies that $P(n)$ is true for all n, completing the proof of the lemma.

We now return to the proof of Theorem 91.

We know that $(a+b)^n$ is the sum of 2^n terms, each of which is the product $\prod \mathbf{q}$ for a list $\mathbf{q} \in Q_n(a,b)$.

We now assume that a and b belong to a number system where the commutative law of multiplication holds. Then in every product $\prod \mathbf{q}$ we can move all the a factors to the left, and conclude that

$$\prod \mathbf{q} = a^{k(\mathbf{q})}b^{n-k(\mathbf{q})}$$

where $k(\mathbf{q})$ is the number of a's that occur in the list $\mathbf{q}$. (For example, if $\mathbf{q} = (a,b,b,b,a,a,b,a,b,b,a,b,a,a,b,b,a)$ then $\prod \mathbf{q} = a^8b^9$.)

So:

$$(a+b)^n = \sum_{\mathbf{q}\in Q_n(a,b)} a^{k(\mathbf{q})}b^{n-k(\mathbf{q})}\,. \tag{21.33}$$

Let us group together, for each k, all the terms corresponding to lists $\mathbf{q}$ that have k a's. To do this, let me define $Q_n(k,a,b)$ to be the set of all lists $\mathbf{q} \in Q_n(a,b)$ such that $k(\mathbf{q}) = k$. Then we can sum first over all $\mathbf{q} \in Q_n(,k,a,b)$, for each k, and then sum over all k. We get

$$(a+b)^n = \sum_{k=0}^{n}\Bigg(\sum_{\mathbf{q}\in Q_n(k,a,b)} a^{k(\mathbf{q})}b^{n-k(\mathbf{q})}\Bigg)\,,$$

that is,

$$(a+b)^n = \sum_{k=0}^{n}\Big(\sum_{\mathbf{q}\in Q_n(k,a,b)} a^{k}b^{n-k}\Big)\,. \tag{21.34}$$

Now, all the terms in the sum $\sum_{\mathbf{q}\in Q_n(k,a,b)} a^kb^{n-k}$ have the same value, namely, a^kb^{n-k}. So the sum $\sum_{\mathbf{q}\in Q_n(k,a,b)} a^kb^{n-k}$ is equal to $\nu_k a^kb^{n-k}$, where ν_k is the number of terms in the sum. And then

$$(a+b)^n = \sum_{k=0}^{n}\nu_k a^kb^{n-k}\,. \tag{21.35}$$

To conclude, we have to determine the numbers ν_k. Clearly, ν_k is the number of members of $Q_n(k,a,b)$, that is, the number of lists $\mathbf{q} = (q_j)_{j=1}^n$ of a's and b's that have k a's.

Now, each list $\mathbf{q} \in Q_n(a,b)$ corresponds to a subset $S(\mathbf{q})$ of the set $\mathbb{N}_n$ as follows: for a list $\mathbf{q} \in Q_n(a,b)$, let $S(\mathbf{q})$ be the set of those indices $j \in \mathbb{N}_n$ such that $q_j = a$. (In other words, a list $\mathbf{q}$ of length n whose entries are a's and b's is determined by the set of those locations j where the entry q_j of $\mathbf{q}$ is a.) In this way, the 2^n lists belonging to $Q_n(a,b)$ correspond to the 2^n subsets of $\mathbb{N}_n$.

And, with this correspondence, if $k \in \mathbb{N} \cup \{0\}$ and $k \leq n$, the lists with k entries equal to a correspond to the subsets of $\mathbb{N}_n$ that have k members, i.e., to the members of $\mathcal{P}_k(\mathbb{N}_n)$. It then follows that the number ν_k of such lists is equal to the cardinality of $\mathcal{P}_k(\mathbb{N}_n)$, that is, to $\begin{pmatrix} n \\ k \end{pmatrix}$.

Hence $\nu_k = \begin{pmatrix} n \\ k \end{pmatrix}$, and (21.35) becomes

$$(a+b)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} a^k b^{n-k} \,, \qquad (21.36)$$

which is the binomial formula. **Q.E.D.**

21.4.1 Some important facts about the binomial formula I: the sum of the binomial coefficients

In the binomial formula, if we plug in $a = 1$, $b = 1$, we get

$$2^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} \,, \qquad (21.37)$$

because, when $a = 1$ and $b = 1$, all the products $a^k b^{n-k} = 1$ are equal to 1.

This identity has been derived from the binomial formula, but both sides have meanings in terms of set counting. So ***there has to be a reason for (21.37) in terms of set counting.*** What is the reason?

Actually, the answer is quite simple: 2^n is the number of subsets of a set A with n members, i.e., the cardinality of the power set $\mathcal{P}(A)$. And $\begin{pmatrix} n \\ k \end{pmatrix}$ is the number of subsets of A that have k members, i.e., the cardinality of $\mathcal{P}_k(A)$.

Since every subset X of A is in $\mathcal{P}_k(A)$ for one and only one k, it is clear that the sets $\mathcal{P}_k(A)$, for $k = 0, 1, \ldots, n$ are pairwise disjoint, and their union is $\mathcal{P}(A)$.

Then

$$\text{card}\Big(\mathcal{P}(A)\Big) = \sum_{k=0}^{n} \text{card}\Big(\mathcal{P}_k(A)\Big) \,,$$

that is

$$2^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} \,.$$

This is the set-theoretic explanation for Formula (21.37).

21.4.2 Some important facts about the binomial formula II: the alternating sum of the binomial coefficients

In the binomial formula, if we plug in $a = -1$, $b = 1$, the left-hand side is zero, because $(1-1)^n = 0$. So the formula becomes

$$0 = \sum_{k=0}^{n} (-1)^k \left(\begin{array}{c} n \\ k \end{array} \right) . \tag{21.38}$$

This identity has been derived from the binomial formula, but both sides have meanings in terms of set counting. So ***there has to be a reason for (21.38) in terms of set counting.*** What is the reason?

Actually, the answer is quite simple. The power $(-1)^k$ is equal to $+1$ when k is even and to -1 when k is odd.

So formula (21.38) actually says:

$$0 = \sum_{k \text{ even}} \left(\begin{array}{c} n \\ k \end{array} \right) - \sum_{k \text{ odd}} \left(\begin{array}{c} n \\ k \end{array} \right) ,$$

that is,

$$\sum_{k \text{ even}} \left(\begin{array}{c} n \\ k \end{array} \right) = \sum_{k \text{ odd}} \left(\begin{array}{c} n \\ k \end{array} \right) . \tag{21.39}$$

If A is a set with n members, then the number $\sum_{k \text{ even}} \left(\begin{array}{c} n \\ k \end{array} \right)$ is the sum of the cardinalities of all the sets $\mathcal{P}_k(A)$ for k even. If we use $\mathcal{P}_{even}(A)$ to denote the set of all subsets of A that have an even number of members, then

$$\mathcal{P}_{even}(A) = \bigcup_{k \text{ even}} \mathcal{P}_k(A) ,$$

and the sets $\mathcal{P}_k(A)$ are pairwise disjoint. So

$$\begin{aligned} \text{card}\Big(\mathcal{P}_{even}(A)\Big) &= \sum_{k \text{ even}} \text{card}\Big(\mathcal{P}_k(A)\Big) \\ &= \sum_{k \text{ even}} \left(\begin{array}{c} n \\ k \end{array} \right) . \end{aligned}$$

Similarly,

$$\begin{aligned}\operatorname{card}\Big(\mathcal{P}_{odd}(A)\Big) &= \sum_{k \text{ odd}} \operatorname{card}\Big(\mathcal{P}_k(A)\Big)\\ &= \sum_{k \text{ odd}} \left(\begin{array}{c} n\\ k\end{array}\right).\end{aligned}$$

So Formula (21.39) just says that

$$\operatorname{card}\Big(\mathcal{P}_{even}(A)\Big) = \operatorname{card}\Big(\mathcal{P}_{odd}(A)\Big)\,,$$

that is, that ***if*** A ***is a finite set, then the number of subsets of*** A ***with an even number of members is equal to the number of subsets of*** A ***with an odd number of members***.

This is a fact that you proved in Problem 54 using purely set-theoretic arguments.

So now we have found the set-theoretic explanation for Formula (21.38).

21.4.3 Some important facts about the binomial formula III: The recursive formula for the binomial coefficients

In Problem (55) you proved that the binomial coefficients $\left(\begin{array}{c} n\\ k\end{array}\right)$ are integers.

And this was done by first proving the formula

$$\left(\begin{array}{c} n+1\\ k\end{array}\right) = \left(\begin{array}{c} n\\ k-1\end{array}\right) + \left(\begin{array}{c} n\\ k\end{array}\right). \tag{21.40}$$

which expresses the binomial coefficients for $n+1$ in terms of the the binomial coefficients for n, and makes it easy to prove by induction that all the binomial coefficients are integers. (The proof is, simply, that if all the binomial coefficients $\left(\begin{array}{c} n\\ k\end{array}\right)$ for a given n are integers, then all the binomial coefficients $\left(\begin{array}{c} n+1\\ k\end{array}\right)$ for $n+1$ are integers as well, because of Formula (21.40). This is the inductive step of the proof. The base step is trivial, because $\left(\begin{array}{c} 1\\ 0\end{array}\right) = \left(\begin{array}{c} 1\\ 1\end{array}\right) = 1$, so all the binomial coefficients for $n=1$ are integers.)

On the other hand, we have also given a totally different proof of the fact that he binomial coefficients are integers, based on set counting: we proved that the binomial coefficients are the cardinalities of certain finite sets (precisely, the sets $\mathcal{P}_k(A)$), and this implies that they are integers.

Since we have two different proofs of the fact that the binomial coefficients are integers, one based on set counting and the other one based on proving Formula (21.40) by purely algebraic means, it is reasonable to ask the following question: ***is there a set-theoretic reason for Formula (21.40)?***

The answer is ***"yes, there is a very simple set-theoretic proof of Formula (21.40)"***.

Here is the proof: Let A be a set with $n+1$ members. Pick a member a if A. Let $B = A - \{a\}$, so B has n members.

As before, let $\mathcal{P}_k(A)$ be the set of all subsets X of A that have k members. Then, if $k > 0$, the members of $\mathcal{P}_k(A)$ are of two kinds: those that have a as a member, and those that do not.

The members of $\mathcal{P}_k(A)$ that do not have a as a member are exactly the subsets of B with k members. So the number of such subsets is $\begin{pmatrix} n \\ k \end{pmatrix}$.

The members of $\mathcal{P}_k(A)$ that have a as a member are obtained by taking subsets of B with $k-1$ members and adding a to them. So the number of these sets is exactly the number of subsets of B with $k-1$ members. So the number of such subsets is $\begin{pmatrix} n \\ k-1 \end{pmatrix}$.

It follows that

$$\text{card}\Big(\mathcal{P}_k(A)\Big) = \begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k-1 \end{pmatrix}.$$

But $\text{card}\Big(\mathcal{P}_k(A)\Big) = \begin{pmatrix} n+1 \\ k \end{pmatrix}$.

So

$$\begin{pmatrix} n+1 \\ k \end{pmatrix} = \begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k-1 \end{pmatrix}.$$

This proves (21.40), and we have found a purely set-theoretic explanation for (21.40).

Problem 62.

1. ***Prove*** that the binomial coefficients satisfy the following symmetry law:

$$\begin{pmatrix} n \\ k \end{pmatrix} = \begin{pmatrix} n \\ n-k \end{pmatrix} \qquad \text{whenever } n, k \in \mathbb{N} \cup \{0\} \text{ and } k \le n \,. \tag{21.41}$$

2. ***Find*** a a purely set-theoretic explanation for (21.41). □

21.4.4 Some important facts about the binomial formula IV: Tartaglia's triangle (a.k.a. Pascal's triangle)

The following famous array of numbers is called by everal names. The most common ones are Tartaglia's triangle, and Pascal's triangle. The array continues indefinitely, but I am only showing the first 11 lines.

$$\begin{array}{ccccccccccccccccccccccc}
 & & & & & & & & & & 1 & & 1 \\
 & & & & & & & & & 1 & & 2 & & 1 \\
 & & & & & & & & 1 & & 3 & & 3 & & 1 \\
 & & & & & & & 1 & & 4 & & 6 & & 4 & & 1 \\
 & & & & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & & & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
 & & & & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 \\
 & & & 1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1 \\
 & & 1 & & 9 & & 36 & & 84 & & 126 & & 126 & & 84 & & 36 & & 9 & & 1 \\
 & 1 & & 10 & & 45 & & 120 & & 210 & & 252 & & 210 & & 120 & & 45 & & 10 & & 1 \\
1 & & 11 & & 55 & & 165 & & 330 & & 462 & & 462 & & 330 & & 165 & & 55 & & 11 & & 1
\end{array}$$

The entries of the array are the binomial coefficients $\begin{pmatrix} n \\ k \end{pmatrix}$. Each row corresponds to one value of n, and you can find which value it is by looking at the second entry of the row from the left, that is, the entry to the right of the leftmost 1.

And, for each row, the entries correspond to the values of k. So, for example, the row for $n = 7$ says that

$$\begin{array}{llll}
\begin{pmatrix} 7 \\ 0 \end{pmatrix} = 1 \,, & \begin{pmatrix} 7 \\ 1 \end{pmatrix} = 7 \,, & \begin{pmatrix} 7 \\ 2 \end{pmatrix} = 21 \,, & \begin{pmatrix} 7 \\ 3 \end{pmatrix} = 35 \,, \\
\begin{pmatrix} 7 \\ 4 \end{pmatrix} = 35 \,, & \begin{pmatrix} 7 \\ 5 \end{pmatrix} = 21 \,, & \begin{pmatrix} 7 \\ 6 \end{pmatrix} = 7 \,, & \begin{pmatrix} 7 \\ 7 \end{pmatrix} = 1 \,.
\end{array}$$

The entries of the array are computed using the recursive formula

$$\begin{pmatrix} n+1 \\ k \end{pmatrix} = \begin{pmatrix} n \\ k-1 \end{pmatrix} + \begin{pmatrix} n \\ k \end{pmatrix} . \tag{21.42}$$

Each entry is the sum of the two entries above it, the one Northwest of it and the one Northeast of it.

For example, if you look at the 84 in the row for $n = 9$, you will ser that

1. $84 = \begin{pmatrix} 8 \\ 3 \end{pmatrix}$.
2. $84 = 28 + 56$.
3. $28 = \begin{pmatrix} 7 \\ 2 \end{pmatrix}$.
4. $56 = \begin{pmatrix} 7 \\ 3 \end{pmatrix}$.
5. So the fact that $84 = 28 + 56$ corresponds to the fact that $\begin{pmatrix} 8 \\ 3 \end{pmatrix} = \begin{pmatrix} 7 \\ 2 \end{pmatrix} + \begin{pmatrix} 7 \\ 3 \end{pmatrix}$, which is a special case of (21.42).

Example 68. Tartaglia's triangle is useful if you want to write the full binomial formula for large exponents.

Let us write the binomial formula for $(a+b)^{11}$. According to the triangle, the formula is

$$\begin{aligned} (a+b)^{11} \quad = \quad & a^{11} + 11a^{10}b + 55a^9b^2 + 165a^8b^3 + 330a^7b^4 + 462a^6b^5 \\ & +462a^5b^6 + 330a^4b^7 + 165a^3b^8 + 55a^2b^9 + 11ab^{10} + b^{11} . \end{aligned}$$

Problem 63.

1. ***Write*** the full Tartaglia triangle up to $n = 14$.
2. ***Verify*** by looking at the rows for $n = 2, 3, 5, 7, 11, 13$ that the following statement is true in all these cases:

   (#) *All the binomial coefficients* $\begin{pmatrix} n \\ k \end{pmatrix}$, *except for* $k = 0$ *and* $k = n$, *are divisible by* n.

3. ***Verify*** by looking at the rows for $n = 4, 6, 8, 9, 10, 12$ that statement (#) is not true in those cases:

4. ***Prove*** that statement (#) is true in general for every prime number n, not just for $n = 2, 3, 5, 7, 11, 13$.

Problem 64. ***Prove*** that for every natural number n the real number x_n given by

$$x_n = (3 + 4\sqrt{7})^n + (3 - 4\sqrt{7})^n$$

is an integer. □

Problem 65. ***Prove*** that for every natural number n

$$\sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix}^2 = \begin{pmatrix} 2n \\ n \end{pmatrix} .$$

(HINT: $(1+x)^n(1+x)^n = (1+x)^{2n}$. Expand the three powers of sums using the binomial formula, and compare the coefficients of x^n. Remember that $\begin{pmatrix} n \\ k \end{pmatrix} = \begin{pmatrix} n \\ n-k \end{pmatrix}$.) □