MATH/COMP61-03 Spring 2014 Notes: January 23rd

Andrew Winslow

1 Lists

Definition. *A* list *is an ordered collection of objects.*

The notation for lists to start with an open parenthesis, then the objects in order separated by commas, then a closed parenthesis. Examples include $(1, 2, 3)$, (x, y, z), and (c, a, b). Since order matters, $(1, 2, 3, 4) \neq (2, 3, 1, 4)$. The objects can be anything, so $(3, \pi, \frac{4}{3}, a)$ is a valid list, as is $(1, 2, (1, 2))$, a list whose third element is also a list.[1] Lists are also sometimes called *tuples*.

Definition. *The* length *of a list is the number of elements in the list.*

The list $(1, 2, 3)$ has length 3, and $(\sqrt{2})$ has length 1. The special case of length-2 list is an *ordered pair*. A list of length k is also sometimes called a k*-tuple*. You've probably seen two-dimensional coordinates specified as ordered pairs of numbers, e.g. a line segment between $(1, 4)$ and $(7, 2)$. Sentences and words are also lists, e.g. "Cats enjoy naps." can be represented by the length-3 list $(\text{Cats}, \text{enjoy}, \text{naps})$ and "Cats" can be represented by the length-4 list $(\text{C}, \text{a}, \text{t}, \text{s})$.

One thing lists are good for is counting objects that themselves are described by multiple parts. A vacation can be described by a 3-tuple (l, s, a), where l is a location (say Miami, Hawaii, or Tokyo), s is the season (say spring, summer, fall, or winter), and a is the activity (say windsurfing or hiking). For instance, $(\text{Miami}, \text{winter}, \text{hiking})$ is a vacation, as is $(\text{Tokyo}, \text{spring}, \text{windsurfing})$.

If we assume we can go anywhere at any time and do anything, then the number of possible vacations is $3 \times 4 \times 2$, that is, the number of locations times the number of seasons times the number of activities.[2] This is a special case of the *Multiplication Rule*:

Theorem (Multiplication Rule)**.** *Consider length-k lists $(c_1, c_2, \ldots, c_k)$ with s_i choices for the element c_i. The total number of possible lists is $s_1 \times s_2 \times \cdots \times s_k$.*

For the previous example, $s_1 = 3$, $s_2 = 4$, and $s_3 = 2$. So the multiplication rule says the number of total vacations is $3 \times 4 \times 2 = 24$. Consider a similar problem where each choice is from the same set of elements:

[1] Listception.

[2] In lecture I said we'd use $\cdot$ for multiplication, and now I'm using $\times$ like a jerk. The reason is that $\times \cdots \times$ is easier to see and understand than $\cdot \cdots \cdot$.

Problem. *How many length-4 lists* (c_1, c_2, c_3, c_4) *are there where* c_1, c_2, c_3, c_4 *are integers with* $1 \leq c_1, c_2, c_3, c_4 \leq 3$*?*

The multiplication rule tells us that the number of such lists is $3 \times 3 \times 3 \times 3 = 3^4$. The situation where each elements of the list is a choice from the same set can be described as a restricted version of the multiplication rule:

Theorem. *Consider length-k lists* $(c_1, c_2, \ldots, c_k)$ *with s choices for each element. The total number of possible lists is* s^k.

Note that the multiplication rule only applies to counting lists where the choice for each element is *independent* from the choice for any other element: any two choices can be made without concern for the other. What if we want to count lists where there is some relationship? The multiplication rule does not apply in this case.

Suppose we want to know how many length-3 lists (c_1, c_2, c_3) exist whose elements consist of integers from 1 to 5 where no integer is used more than once. So $(3, 5, 4)$ is ok, as is $(1, 2, 5)$, but $(1, 4, 1)$ and $(3, 3, 3)$ are not. This problem can be posed as a sequence of choices, where each choice restricts later choices:

1. Select the first element c_1 with $1 \leq c_1 \leq 5$.
2. Select the second element c_2 with $1 \leq c_2 \leq 5$ and $c_2 \neq c_1$.
3. Select the third element c_3 with $1 \leq c_3 \leq 5$ and $c_3 \neq c_1$ and $c_3 \neq c_2$.

At Step 1, there are 5 options. At Step 2, there are 4 options, since c_1 is forbidden from being picked. At Step 3, there are 3 options, since c_1 and c_2 are forbidden from being picked and $c_1 \neq c_2$. Each sequence of valid choices gives a valid list, and every valid list can be obtained by a sequence of valid choices, since any valid list obeys the restriction that $c_2 \neq c_1$, $c_3 \neq c_1$, and $c_3 \neq c_2$ because no element appears twice in the list. So the total number of such lists is $5 \times 4 \times 3 = 60$.

Now consider the more general case, where we want to know how many length-k lists $(c_1, c_2, \ldots, c_k)$ there where each element is distinct and selected from the integer from 1 to n. We can use a similar sequence of choices as for the special case of $k = 3$, $n = 5$ we already saw. There are n options for the first choice c_1, $n - 1$ options for the second choice (cannot reuse c_1), $n - 2$ options for the third choice (cannot reuse c_1 or c_2), etc. This leads to a new rule:

Conjecture. *Consider length-k lists* $(c_1, c_2, \ldots, c_k)$ *where* $1 \leq c_i \leq n$ *for each* c_i *and no two elements are the same. There are* $n \times (n-1) \times (n-2) \times \cdots \times (n-(k-1))$ *such lists.*

The total number of any set of objects should be a non-negative integer ("-1 apples" does not make sense). Notice that for some values of k and n, for instance $n = 3$ and $k = 5$, the theorem says that the total number of lists is negative – what the heck! The situation where $n = 3$ and $k = 5$ is asking for the number of lists of length five using distinct integers between 1 and 3, but there is no such list! So our conjecture is wrong in these cases, namely any cases where the number of options for the last choice is less than 1. Here's the revised rule:

Theorem. *Consider length-k lists $(c_1, c_2, \ldots, c_k)$ where $1 \leq c_i \leq n$ for each c_i and no two elements are the same. If $n-k \geq 0$, there are $n \times (n-1) \times (n-2) \times \cdots \times (n-(k-1))$ such lists. Otherwise, there are 0 such lists.*

Notice that if $n-k=0$, then the total number of such lists is $n \times n-1 \times \cdots \times 2 \times 1$. Moreover, every number from 1 to n appears in each list. For instance, the lists for $n = k = 3$ are:

$$\begin{array}{cc} (1,2,3) & (1,3,2) \\ (2,1,3) & (2,3,1) \\ (3,1,2) & (3,2,1) \end{array}$$

Because each number appears exactly once in the list, the list describes an ordering on the numbers 1 through n. We call an ordering of a set of things a *permutation*:

Definition. *A list $(c_1, c_2, \ldots, c_k)$ of k objects, where each object appears once in the list is a* permutation *of the objects $c_1, c_2, \ldots, c_k$.*

For instance, $(1,2,3,4,5)$ and $(3,4,1,2,5)$ are both permutations of the same set of objects. This is all leading up to a nice question about how many ways there are to order a set of objects:

Problem. *How many permutations of n objects are there?*

As you might imagine, people have asked this question before. The answer is $n!$.[3] What is $n!$? Read on to find out...

2 Factorial

People who studied permutations found this definition useful:

Definition. *For any integer $n \geq 1$, n* factorial *is $n \times (n-1) \times \ldots 2 \times 1$ and is written $n!$.*

Does this look familiar? Here's the previous theorem about lists of objects restricted to the special case of $n = k$:

Theorem. *Consider length-n lists $(c_1, c_2, \ldots, c_n)$ where $1 \leq c_i \leq n$ for each c_i and no two elements are the same. There are $n \times (n-1) \times (n-2) \times \cdots \times 1$ such lists.*

Now here's the same theorem written using n factorial:

Theorem. *Consider length-n lists $(c_1, c_2, \ldots, c_n)$ where $1 \leq c_i \leq n$ for each c_i and no two elements are the same. There are $n!$ such lists.*

[3] The exclamation point is not my enthusiasm. It has a formal definition when placed after non-negative integer quantity.

So the number of permutations of the numbers 1 through n is $n!$. Now suppose we had some other objects whose permutations we wanted to study, like cats. We could give each cat a nametag with an integer on it, i.e. the first cat gets a nametag "Cat 1", the second "Cat 2" and so on. Placing the cats in a line then gives a permutation of cats and a corresponding permutation of the numbers 1 through n. For each cat permutation there is a unique number permutation and vice versa. So the number of cat permutations is the same as the number of permutations of the integers 1 through n. This gives us a general theorem for n objects (be them cats or something else):

Theorem. *There are $n!$ permutations of n objects.*

3 Adding and Multiplying Lots of Things

This is an aside about the notation for adding and multiplying lots of things together when they can be described compactly. In a previous course, you may have seen something like the following:

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

The big symbol is a capital sigma (greek letter). More generally:

Definition. *Given integers j, k with $j \leq k$,*

$$\sum_{i=j}^{k} i = j + (j+1) + (j+2) + \cdots + (k-1) + k$$

That is, $\sum_{i=j}^{k}$ is the sum of all the things from from j to k. What about the products of all things from j to k? The choice of **s**igma as the symbol for **s**ummation is because they start with the same letter. Then naturally we use a capital **p**i for the **p**roduct:

Definition. *Given integers j, k with $j \leq k$,*

$$\prod_{i=j}^{k} i = j \times (j+1) \times (j+2) \times \cdots \times (k-1) \times k$$

The special case where $j = 1$ and $k = n$ is:

$$\prod_{i=1}^{n} i = 1 \times 2 \times \cdots \times n$$

With this notation, n factorial can be described in a compact way:

$$n! = \prod_{i=1}^{n} i$$

4 Sets

Definition. *A* set *is a repetition-free, unordered collection objects.*

The notation for sets is to start with an open curly brace, then the objects in some order, then a closed curly brace. Examples include $\{1, 2, 3\}$, $\{x, y, z\}$, and $\{c, a, b\}$. Since order does not matter, $\{1, 2, 3, 4\} = \{2, 3, 1, 4\}$. Since sets do not have repetitions of the same object, putting an object in a set more than once has no effect. For instance, $\{1, 2, 3\} = \{1, 1, 2, 3\} = \{1, 2, 3, 1, 2, 3\}$. Like with lists, the objects can be anything, so $\{3, \pi, \frac{4}{3}, a\}$ is a valid set, as is $\{1, 2, \{1, 2\}\}$, a set of three elements with an element that's also a set.[4]

Definition. *The* cardinality *of a set is the number of elements in the set.*

The notation for the cardinality of a set is a pair of vertical bars around the set. The cardinality of $\{1, 2, 3\}$ is 3, and is denoted $|\{1, 2, 3\}| = 3$. Another example is $|\{1, 1, 2, 2, 3, 3, 4, 4\}| = |\{\pi, \pi^2, \pi^3\}|$. The cardinality of a set is a non-negative integer if the set is finite, such as $\{1, 2, 3\}$, or infinite if the set is is infinite, such as the integers.

Speaking of the integers, recall our early attempt to define the integers:

Definition. *An* integer *is a number in the infinite set* $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Now that we have defined sets, this definition makes sense. We define $\mathbb{Z}$ as shorthand for the integers. There are other infinite sets that come up naturally, like the natural numbers:

Definition. *A* natural number *is an integer* n *with* $n \geq 0$.

Natural numbers can also be defined using set notation as we did with integers:

Definition. *A* natural number *is a number in the infinite set* $\mathbb{N} = \{0, 1, \ldots, \}$.

I've used the ellipsis (the dots ...) in this an previous lectures without a definition. This is mathematically naughty – everything should be defined before usage. Unfortunately, "..." is one of those things like integers that is easier to leave as common sense for now. Ellipsis simply means "keeping going on like this" in situations where "like this" is unambiguous.

Going back to sets, there are symbols used to denote short English phrases, like $\Rightarrow$ means "only if". The most important one for sets is $\in$, which means "is an element of", as in "$3 \in \mathbb{Z}$". This can be used in theorems:

Theorem. *If* $n \in \mathbb{N}$*, then* $n \in \mathbb{Z}$.

Or even more compactly:

Theorem. $n \in \mathbb{N} \Rightarrow n \in \mathbb{Z}$

[4] Setception.

This is looking really clean! Notice how we have a theorem stated entirely in symbols (*symbolically*). Because these symbols have been defined, there is no ambiguity about what the theorem states, and the entire theorem can be written using just six characters. The negation of $\in$ is $\notin$, meaning "is not an element of", as in $-5 \notin \mathbb{N}$.

Sets can be defined by listing off the elements, a la $\{1, 2, 3\}$ or $\{0, 1, 2, \ldots\}$, but in some cases this tedious at best and often ambiguous. *Set-builder notation* is generic and powerful way to define sets. It usually looks like

$$\{\text{variable} \ \in \ \text{set} \ : \ \text{condition}\}$$

For example, the odd integers are written:

$$\{n \in \mathbb{Z} : 2 \mid (n + 1)\}$$

and the integers from 1 to 10 are written:

$$\{n \in \mathbb{Z} : 1 \leq n \leq 10\}$$

and the natural numbers are written:

$$\{n \in \mathbb{Z} : 0 \leq n\}$$

There are usually many ways to define a set with set-builder notation. All are equal in the eyes of mathematicians – with slight preference to simpler definitions or those that highlight specific structure in the set. Sets are bags of objects, and many interesting questions about sets involve the relationships between two sets, like whether one contains another:

Definition. *A set A is a* subset *of a set B, written $A \subseteq B$, provided for each element $x \in A$, $x \in B$.*

and equivalently:

Definition. *A set B is a* superset *of a set A, written $A \subseteq B$, provided for each element $x \in A$, $x \in B$.*

For instance, $\{1, 2\} \subseteq \{1, 2, 3, 4\}$ and $\mathbb{N} \subseteq \mathbb{Z}$. Every set is also a subset and superset of itself. A set containing nothing is the *empty set*, written $\emptyset$ or $\{\}$. The book prefers the first notation, but I prefer the second when I write in analog, as the first one can be confused with Φ given sufficiently bad handwriting.[5] You can use whichever you like.

5 Quantifiers

It's common to want to make a statement about a whole set of things, like when defining prime integers:

[5] E.g. mine.

Definition. *An integer n is* prime *provided that $1 < n$ and for every $a \in \mathcal{Z}$ with $1 < a < n$, $a \nmid n$.*

The "for every" is what I'm talking about. It's a claim about all possible a having some condition. Alternatively, there's a claim about the existence of at least one a having some condition:

Definition. *An integer n is* composite *provided that $1 < n$ and there exists an $a \in \mathcal{Z}$ with $1 < a < n$ and $a \mid n$.*

For this definition, the "there exists" is what I'm talking about. It's a claim about the existence of an a that divides n. These little phrases "for every" and "there exists" show up a lot, so much that we have symbols for them, just like for "only if" ($\Rightarrow$), "if and only if" ($\Leftrightarrow$), "is an element of" ($\in$), "is a subset of" ($\subseteq$), etc. For these two phrases, we use $\exists$ ("there exists") and $\forall$ ("for every").

These symbols can be used whereever we like to replace these phrases and formalize definitions, statements, etc. Prime and composite can be redefined as such:

Definition. *An integer n is* prime *provided that $1 < n$ and $\forall a \in \mathbb{Z}$ with $1 < a < n$, $a \nmid n$.*

Definition. *An integer n is* composite *provided that $1 < n$ and $\exists a \in \mathbb{Z}$ with $1 < a < n$ and $a \mid n$.*

We can go further with set builder notation to define the sets that n and a come from:

Definition. *An $n \in \mathbb{N}$ is* prime *provided that $1 < n$ and $\forall a \in \{a \in \mathbb{Z} : 1 < a < n\}$, $a \nmid n$.*

Definition. *An $n \in \mathbb{N}$ is* composite *provided that $1 < n$ and $\exists a \in \{a : \mathbb{Z} : 1 < a < n\}$ such that $a \mid n$.*

Notice that all these symbols and notation make things more concise and precise, but not necessarily easier to read. In general, mixing English and symbols into the most clear and understandable is the goal: use concise notation when excessive wordiness is hard to read, and English when excessive dense symbolic notation is hard to read.

Back to quantifiers, the last thing to cover is a neat relationship between negations of statements using $\exists$ and $\forall$. Consider the statement $A =$ "$\forall a \in \mathbb{Z}$ with $1 < a < n$, $a \nmid n$" The negation of the statement (the statement that is true iff A is false) is $\neg A =$ "$\exists a \in \mathbb{Z}$ with $1 < a < n$, $a \mid n$". In general, negating a statement of the form "$\forall a(\text{claim about a})$" gives the statement "$\exists a(\text{negation of claim about a})$". Similarly, negating a statement of the form "$\exists a(\text{claim about a})$" gives the statement "$\forall a(\text{negation of claim about a})$".