MAT344 Lecture 1

2019/May/7

1 Announcements

1. Make sure you have access to quercus.
2. Enroll in a tutorial (the caps will be increased and a fourth tutorial likely added).
3. Read the Syllabus and Study tips (also uploaded to https://www.math.toronto.edu/balazse/2019_Summer_MAT344/).
4. Read Chapter 1 of the textbook [KT17]. It is an easy and fun read, and explores many of the questions that we will study later in the class.
5. Note: for some reason the textbook .pdf and print versions numbers differ slightly from the (more interactive) html version. When using references, we will refer to the .pdf version.
6. Problem set 1 will be sent out later today.

2 This week

This week, we are talking about

1. Basic counting techniques,
2. Permutations,
3. Combinations

3 Strings (Chapter 2.1 in [KT17])

Exercise 3.1 ([Bog04], Chapter 1.2 Problem 6)**.** *An ice cream parlor offers 12 different flavors of ice cream, and triple decker cones are made in homemade waffle cones. Having chocolate ice cream as the bottom scoop is different from having chocolate ice cream as the top scoop. How many different triple decker cones of ice cream are available?*

Solution: We have 12 choices for all of the bottom, middle, and top scoops, and if two sequence of choices differ at any point, they result in different triple decker ice cream cones. So we have $12 \cdot 12 \cdot 12 = 1728$ different kinds of triple decker cones.

The above problem is a typical one that we will encounter in this class. We are asked "How many...", and with some logic we come up with a number. After solving a problem, a mathematician will ask themselves: what other problems will we be able to solve with this method? To help with this, we use abstraction: we strip away irrelevant parts of the problem and introduce terminology for the parts that matter.

For instance, rather than thinking about flavors in ice cream, we number the flavors:

Definition 3.2. *Combinatorialists like to count things, so the set* $\{1, 2, \ldots, n\}$ *appears a lot. So we use the shorthand* $[n]$ *for it.*

Then instead of thinking of the bottom, middle and top scoops, we number the positions as well:

Definition 3.3. *Let X be a set. An **X-string of length n** is a function $s : [n] \to X$. Alternatively, we will say that a string is a sequence of elements of X, and we'll often write $s = x_1x_2 \dots x_n$. We also refer to strings as **words** in an alphabet X.*

We will use strings as a tool for modeling counting problems. Many times, we can translate a counting question to a question that is about counting strings. Why is this a good idea? Strings are really easy to count:

Theorem 3.4. *The number of X-strings of length n is $|X|^n$.*

Before proceeding to the proof of our first Theorem (or any Theorem, for that matter), it is good practice to perform a sanity check. The ice cream problem in the beginning asked us how many triple-decker cones of ice cream are there if there are 12 flavors. Translating this into the language of strings, this is asking us about [12]-strings of length 3. The formula in Theorem 3.4 predicts the number to be $|[12]|^3 = 12^3 = 1728$, which agrees with what we found directly.

Proof of Theorem 3.4. Am X-string of length 1 is just an element of X, and X has $|X|$ many elements. Now assume that the number of X-strings of length k is $|X|^k$. An X-string of length $k+1$ is an X-string of length k followed by an X-string of length 1. Therefore there are $|X|^{k+1}$ many $|X|$-strings of length $k+1$, and we are done by induction.

Q.E.D.

During the course of the proof, we implicitly used two basic counting principles. Let A and B be disjoint sets (recall this means that A and B have no elements in common). Recall that the union of two sets $A \cup B$ consists of elements that are either in A or B, while the product $A \times B$ consists of ordered pairs (a, b) such that $a \in A, b \in B$.

1. The **addition principle** says that $|A \cup B| = |A| + |B|$.
2. The **multiplication principle** says that $|A \times B| = |A| \cdot |B|$.

Example 3.5. *Let $A = \{x, y\}, B = [3]$. Then $|A| = 2, |B| = 3$. We have $A \cup B = \{x, y, 1, 2, 3\}$ and $|A \cup B| = 5$. We have $A \times B = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$, and $|A \times B| = 6$.*

Remark 3.6. *The set of functions from a set X to another set Y is often denoted Y^X. Why is this a good notation?*

Example 3.7 ([KT17], Example 2.2)**.** *A machine instruction in a 32-bit operating system is a bit string of length 32, or, in our language, a [2]-string of length 32. There are 2^{32} many of these.*

The next problem illustrates that Theorem 3.4 is not flexible enough to handle all string-counting problems on the nose:

Exercise 3.8. *Standard passenger vehicle licence plates in Ontario are four letters in the English alphabet, followed by three digits. How many possible licence plates are there?*

But if we first break the problem down to simpler parts, where Theorem 3.4 is applicable, and use it together with the addition and multiplication principles, we can solve many problems.

Solution: Consider the four letters first. By Theorem 3.4, there are $26^4 = 456976$ different sequences of four letters. Similarly, there are $10^3 = 1000$ possibilities for the three digits. By the product principle, there are $456976 \cdot 1000 = 456976000$ possible licence plates.

At this point, you might wonder what good it is to be able to count things, what will we do with these numbers? The next problem illustrates a potentially important application:

Exercise 3.9 ([KT17], Exercise 2.9.3)**.** *Matt is designing a website authentication system. He knows passwords are most secure if they contain letters, numbers, and symbols. However, he doesn't quite understand that this additional security is defeated if he specifies in which positions each character type appears. He decides that valid passwords for his system will begin with three letters (uppercase and lowercase both allowed), followed by two digits, followed by one of 10 symbols, followed by two uppercase letters, followed by a digit, followed by one of 10 symbols. How many different passwords are there for his website system? How does this compare to the total number of strings of length 10 made from the alphabet of all uppercase and lowercase English letters, decimal digits, and 10 symbols?*

Solution: Following the logic of the previous problem, there are $(2 \cdot 26)^3 \cdot 10^2 \cdot 10 \cdot 26^2 \cdot 10 \cdot 10 = 9505100800000 \approx 9 \cdot 10^{13}$ with Matt's conventions, whereas if we allow letters, digits and symbols at all of the 10 places, we get $(2 \cdot 26 + 10 + 10)^{10} = 3743906242624487424 \approx 4 \cdot 10^{19}$ passwords, roughly 400000 times more than with Matt's convention!

4 Permutations (Chapter 2.2 in [KT17])

We have already seen some limitations of using strings to model counting problems in the previous section. Imagine a situation where four people stand in a line. Representing the four people by numbers, this corresponds to counting certain [4]-strings of length 4. There are $4^4 = 256$ of these in total, but most of them are not useful for us, since we want each number to appear exactly once. Let's think of it in a different way. Any of the 4 people can stand in the first position, then any of the remaining 3 people can be second, then either of the remaining 2 people can fill the third spot, and we have no choice about the last position. Altogether this says that we have $4 \cdot 3 \cdot 2 \cdot 1 = 24$ choices (notice how different this number is from 256).

Definition 4.1. *An X-string $s = x_1 x_2 \dots x_n$ is called a **permutation** if all n characters used in s are distinct.*

Definition 4.2. *When n is a positive integer, we define $n!$ (n factorial) by*

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1.$$

and we set $0! = 1$.

The discussion above is easily generalized to the following result:

Proposition 4.3. *Let X be a set with $|X| = n$. There are $n!$ many ways of ordering the elements of X.*

With a little modification, this can be used to answer more general questions:

Definition 4.4. *Let $n \geq k \geq 0$. We define*

$$P(n,k) = \frac{n!}{(n-k)!} = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+2) \cdot (n-k+1).$$

Theorem 4.5. *[[KT17], Proposition 2.5] If X is an n-element set and k is a positive integer with $n \geq k$ then the number of X-strings of length k that are permutations is $P(n,k)$.*

As before, in some cases we have to be clever about using Theorem 4.5:

Exercise 4.6. *We want to sit 5 out of 10 people at a round table, where it does not matter where you sit, only who your left-hand and right-hand neighbors are (in other words, rotating around the table results in the same configuration, but this is not true for reflections). In how many ways can they sit down?*

Solution: Consider the situation where 5 out of 10 people are forming a line. Theorem 4.5 implies immediately that there are $P(10,5) = \frac{10!}{5!} = 30240$ ways of doing this. Now imagine that we arbitrarily pick a chair, and declare it the first chair. Then effectively we are making people form a line, so there are 30240 many ways. But since the first choice of the chair does not matter, we counted each case 5 times. So there are 6048 many ways of sitting the people around the table.

The preceding problem illustrates an important technique. Often it is easier to **overcount** something, and then figure out how much we overcounted by.

Exercise 4.7 (Fermat's little theorem)**.** *If you have seen some number theory or abstract algebra, you may know that if p is a prime and k is a positive integer, then $k^p - k$ is divisible by p. We will give a proof of this theorem using combinatorial reasoning.*

1. *Suppose we have beads of k different colors. We are putting p many of them on a string. In how many ways can we do this?*
2. *How about if we want to use at least 2 different colors? (**Hint:** It is a lot easier to count those strings of beads where we have only used 1 color)*

3. *Now we tie the two ends of the string together, forming a necklace. Cyclic rotations of sequences may result in the same necklace. How much did we overcount by? Make sure to use the fact that p is a prime.*

4. *How does this show that $k^p - k$ is divisible by p?*

Exercise 4.8 ([Gui18], Exercise 1.2.5)**.** *In chess, a rook attacks any piece in the same row or column as the rook, provided no other piece is between them. In how many ways can eight indistinguishable rooks be placed on an 8×8 chessboard so that no two attack each other? What about eight indistinguishable rooks on a 10×10 board?*

Exercise 4.9 ([Bog04], Chapter 1.2 Problem 7)**.** *The idea of a function is ubiquitous in mathematics. A function f from a set S to a set T is a relationship between the two sets that associates exactly one member $f(x)$ of T with each element x in S.*

(a) Using $f, g, \ldots,$ to stand for the various functions, write down all the different functions you can from the set $[2]$ to the set $\{a, b\}$. For example, you might start with $f(1) = a, f(2) = b$. How many functions are there from the set $[2]$ to the set $\{a, b\}$?

(b) How many functions are there from the three element set $[3]$ to the two element set $\{a, b\}$?

(c) How many functions are there from the two element set $\{a, b\}$ to the three element set $[3]$?

(d) How many functions are there from a three element set to a 12 element set?

*(e) The function f is called **one-to-one** or an **injection** if whenever x is different from y, $f(x)$ is different from $f(y)$. How many one-to-one functions are there from a three element set to a 12 element set?*

References

[Bog04] Kenneth P. Bogart. *Combinatorics Through Guided Discovery.* Open access, 2004. Available at http://bogart.openmathbooks.org/. 1, 4

[Gui18] David Guichard. *Combinatorics and Graph Theory.* Open access, 2018. Available at https://www.whitman.edu/mathematics/cgt_online/book/. 4

[KT17] Mitchel T. Keller and William T. Trotter. *Applied Combinatorics.* Open access, 2017. Available at http://www.rellek.net/appcomb/. 1, 2, 3