Lecture 1: 205 recap, sum rule, and the union bound

Discrete Structures II (Summer 2018)
Rutgers University
Instructor: Abhishek Bhrushundi

References: Relevant parts of chapters 1,3,4,5, and 15 of the Math for CS book

1 What is the course about?

The course is about counting and probability basics. These tools are helpful to know as a computer scientist, no matter which subfield of CS you get into. I will post some reading material which gives examples of applications of counting and probability in CS. To get an idea about the topics that will be covered in this course check out the syllabus PDF on Sakai.

2 Lecture notes

Note that the purpose of the lecture notes is to supplement the lectures, and not to replace them! You will find that the lecture notes are a barebone sketch of what actually happened in the lecture. My main motivation to type these out is

1. to let students who missed the lecture get an idea as to what was covered in class (and how awesome it was, and why they shouldn't miss a class again), and
2. to stimulate the associative memory of students who did attend the class, serving as a sort of a refresher.

The notes might have typos/minor mistakes (hopefully not major stuff), so please feel free to point them out.

3 How to do well in this course?

First and foremost, attend the lectures and recitations, and bug your instructor and TAs with any doubts/questions you have. Second, practice, practice, and practice! The *Mathematics for Computer Science* book has a whole bunch of practice problems. Additionally, you'll have enough problems to ponder over between your HWs, Quizzes, and practice problem sets.

Oh, and we have office hours (4 of them in a week!) so make sure you drop by and make use of them! You can also discuss problems (not HW problems though) on Piazza!

4 Getting ready: a 205 recap

We will be using a lot of 205 concepts in this course so the first thing you want to do is to brush up on those concepts if you feel they are getting rusty! In this lecture, we will try to do a crash course on the essential 205 concepts. You'll also get a glimpse into future topics involving counting!

4.1 Set theory

Without getting into super-formal definitions, let's just say that a set is a *collection* of objects. See if you can remember what these mean:

- Commonly used sets: $\mathbb{R}, \mathbb{Z}, \mathbb{N}, \mathbb{Q}, \mathbb{C}$, etc.
- Set operations: $X \cap Y, X \cup Y, X \setminus Y, X \times Y, |X|, 2^X, X^c$.

Here are some exercises to test you:

Question . Is it always the case that for two sets X and Y, $X \setminus Y = Y \setminus X$? If not, give a counterexample!

If X is a set then 2^X or $powerset(X)$ is called the *power set* of X and it is the set of all subsets of X. For example, if $X = \{1, 2\}$, then $2^X = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Often, we will use the *set builder* notation to define a set, e.g. $X = \{n \in \mathbb{N} |$ n is a prime$\}$. Here are some more problems to test yourself:

Question . Let $A = \{n \in \mathbb{N} : \ n^2 < 49\}$ and $B = \{n \in \mathbb{N} : \$ n is a prime$\}$. Find $A \cap B, A \cup B, A \setminus B, A \times B$.

$A \times B$ is the cartesian product and is the set of all pairs (a, b) where $a \in A, b \in B$. Notice that these are ordered pairs, unlike the set $\{a, b\}$ which has no innate order. One can extend this to the n-fold cartesian product: $A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) | \ a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$.

The complement of a set A denoted by A^c only makes sense if you know what *universe* A is inside. For example, the set $1, 2$ could be inside the universe $\mathbb{N}$ or the universe $\mathbb{Z}$. Usually it is clear from context what the universe is. For example, if $A = \{1, 2, 3\}$ is a subset of the universal set $S = \{1, 2, 3, 4, 5\}$, then A^c, the complement, is $\{4, 5\}$.

Sometimes it's useful to represent sets visually. This can be done using *Venn diagrams*. In a Venn diagram, every set is represented by a circle, and the intersection between two sets can be represented by showing the circles corresponding to the sets as overlapping. On the other hand if two sets are disjoint, then one can represent that as two non-overlapping/non-intersecting circles. It's useful to bound the sets inside a large rectangle that represents the universe inside which the sets live.

Now let's test your knowledge on the above:

Question . A school has 200 students. 25 of them like both CS and Math, 100 of them like CS, and 50 of them like Math. How many of the students like neither of the two subjects?

4.2 Functions

A function from set A to set B, denoted by $f : A \to B$, "associates" with EVERY $a \in A$ some elememt $b \in B$. Read that again: for EVERY $a \in A$. A is called the domain, and B the codomain. We say that f *maps* the elements in A to elements in B. Note again, it maps EVERY element in A to something in B – there cannot be elements in A that f does not map to an element in B. Of course, two elements in A, say a_1 and a_2 could get mapped to the same $b \in B$. That's totally fine!

When we write $f(a) = b$ for some $a \in A$ and $b \in B$ we mean that a if mapped by f to b. For example, let us define the function f that maps $\mathbb{R}$ to $\mathbb{R}$ (i.e., $f : \mathbb{R} \to \mathbb{R}$) as follows:

$$f(x) = 4 \cdot x.$$

This means that the real number x is mapped to the real number $4 \cdot x$. 2 is mapped to 4, 4 is mapped to 16, etc. There are different "types" of functions:

1. Injective functions: A functon $f : A \to B$ is injective if for $a_1, a_2 \in A$ (where $a_1 \neq a_2$, i.e. they are not the same element), $f(a_1) \neq f(a_2)$. This means no two elements in A get mapped to the same $b \in B$ by f. See if you can prove this: if $f : A \to B$ is injective then it MUST be the case that $|B| \geq |A|$. Example $f(x) = 4 \cdot x$ where $f : \mathbb{R} \to \mathbb{R}$.

2. Surjective functions: A function $f : A \to B$ is surjective if for every $b \in B$ there is some $a \in A$ such that $f(a) = b$, i.e. some $a \in A$ is mapped to b by f. No $b \in B$ is left alone!
   You can check that if f is surjective then it MUST be the case that $|A| \geq |B|$. Examples of functions that are surjective: $f : \mathbb{Z} \to \mathbb{N}$, $f(x) = |x|$ (absolutve value of x).

3. Bijective functions: If a function is both surjective and injective, then it is a bijective function! If $f : A \to B$ is bijective, what can you say about the relation between $|A|$ and $|B|$?

Sometimes we will use the names *injection, surjection, and bijection* instead of injective function, surjective function, and bijective function.

4.3 Propositions, predicates, axioms, rules of logic, and proofs

Whenever we "do" mathematics, we implicitly deal with the following "entities" from logic:

1. *Proposition*: A proposition is a statement or an assertion that may be true of false (depending on our assumptions). For example, *Every number n has a number larger than it* is a proposition (and it's a true proposition, assuming we are dealing with, say, real numbers), and 4 *is a prime number* is also a proposition, although it's a false one ($4 = 2 \times 2$).

2. *Axioms*: These are our basic assumptions that we make about mathematical objects: for example, if A is a subset of $\{1, 2, \ldots, n\}$, either the number 1 is in A or it's not in A — it cannot both be in and not be in A, or the fact that adding any number to zero gives you back the same number. These are things we just assume and don't try to prove — these are examples of axioms!

3. *Predicate*: Simply put, a predicate is a proposition that has variables in it. For example, X *is divisible by* 2 is a predicate. We cannot say whether it's true or false unless we specify

what X is, so in some ways it's like a function — it's "output" or "value" depends on what "input" you feed it! If $X = 4$, then it becomes true, but if $X = 3$, it's false!

4. *Quantifiers*: You can convert a predicate into a proposition by adding quantifiers. For example, the above predicate becomes a proposition if I add the "for all" quantifier: $\forall X \in \mathbb{N}$, *X is divisible by 2.* Is this proposition true or false?
   You can also add the "there exists" quantifier: $\exists X \in \mathbb{N}$, *X is divisible by* 2. (Is this true or false?).

5. *Rules of logic*: These are rules that we use to go from a set of propositions and axioms to a new proposition. For example, if I have that the proposition $P \implies Q$ is true and have P as an axiom, then together they imply that the proposition Q is true. I wouldn't list all the rules of logic here. You can find a comprehensive list and discussion in Rosen's book (Discrete Math and Its Applications) or in the Mathematics for Computer Science book (See the reading suggestions on Sakai/the course webpage).

6. *Proofs*: A proof starts out with the axioms and other assumptions, and at every step obtains a new proposition from the axioms, assumptions, and previously obtained propositions, using the rules of logic.

4.4 A glimpse into the zoo of different types of proofs

There are different styles of proof that you would have seen in 205. Here are some:

1. *Direct proof*: If you want to prove $P \implies Q$, the simplest way to do so is to assume P is true and then derive/prove Q from P. For example, if you want to prove the following:

   $$1 \leq x \leq 2 \implies x^2 - 3x + 2 \leq 0,$$

   what you can do is to assume that x is between 1 and 2 (inclusive), observe that $x^2 - 3x + 2 = (x-2)(x-1)$ and that, under the assumption, $(x-2) \leq 0$ and $(x-1) \geq 0$, and thus $x^2 - 3x + 2 = (x-2)(x-1) \leq 0$.

2. *Proof by contrapositive*: Instead of directly proving that $P \implies Q$, you prove the contrapositive, i.e, $\neg Q \implies \neg P$, which is a logically equivalent statement. For example, if you want to show that if r is irrational then so is $\sqrt{r}$, you can show the contrapositive:

   $$\text{If } \sqrt{r} \text{ is rational, then so is } r.$$

   If $\sqrt{r}$ is rational, then $\sqrt{r} = a/b$ (for positive integers a and b), and so $r = a^2/b^2$, which means that r is rational.

3. *Proof using a case analysis*: Say you want to show that the function $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = |x+2| - |x-3|$ always takes a value in the interval $[-5, 5]$. Recall that $|x| = x$ if $x \geq 0$, and $|x| = -x$ if $x < 0$. Thus, it makes sense to analyze the behavior of $f(x)$ for different cases depending on the values of x. For example, in the first case we will look at all values of x where $(x+2) < 0$ but $(x+3) \geq 0$. The only value of x that satisfies these conditions is $x = -3$, and in this case $f(x)$ becomes $-x - 2 - x + 3 = 1$, which is in the interval $[-5, 5]$. One can similarly look at other cases and prove the statement for each of the cases.

4. *Proof by contradiction*: If you want to show that a statement/proposition P is true, you assume for the sake of contradiction that P is false, and use that to arrive at some contradiction (a contradiction to one of your axioms or the assumption you started out with). For example, if you want to prove that $\sqrt{2}$ is irrational, you can prove this using proof by contradiction: assume $\sqrt{2}$ is rational and thus $\sqrt{2} = a/b$ such that a and b are positive integers that don't share any common divisors. Then $a^2 = 2 \cdot b^2$. But this means that a^2 is a perfect square that is also even, and so a itself must be even (why?). This means 4 divides a^2, and thus 4 also divides $2 \cdot b^2$ (since $a^2 = 2 \cdot b^2$). This would mean that b^2 is even and thus b is even. So we have shown that both a and b are even, which contradicts the assumption that a and b have no common divisors. Thus, $\sqrt{2}$ cannot be rational.

5. *Proof by weak induction*: Induction is useful for proving statements/propositions of the form

$$\forall n \in \mathbb{N},\ P(n) \text{ is true},$$

where $P(n)$ is a predicate on natural numbers. The idea is to first prove that $P(0)$ is true (this is called the base case. [1]), and then showing that for every $n \geq 0$, $P(n)$ implies $P(n+1)$ (this is the induction step).
For example, to show that the sum of the numbers from 0 to n is $n(n+1)/2$, for all $n \geq 0$, we first observe that the base case ($n = 0$) is trivially true. For the induction step, let n some arbitrary integer greater than 0, and suppose that the sum of 1 to n is $n(n+1)/2$. We will use this to show that the sum of numbers from 1 to $n+1$ is $(n+1)(n+2)/2$, thereby finishing the proof. To see this, note that $1+2+\ldots+n+n+1 = (1+2+\ldots+n)+n+1 = (n(n+1)/2)+(n+1)$, where the last step follows from the inductive assumption. Thus, $1+2+\ldots+n+1 = (n(n+1)/2)+(n+1) = (n+1)(n+2)/2$, and this finishes the proof.

6. *Proof by strong induction*: Sometimes proofs using weak induction can get pretty nasty, and in such cases strong induction comes in handy. Strong induction works exactly the same as way as weak induction except the induction step: in strong induction we have to prove that for all $n \in \mathbb{N}$,$P(0) \wedge P(1) \wedge \ldots P(n) \implies P(n+1)$, i.e. we can now assume not only $P(n)$, but all of $P(0), P(1), P(2), \ldots, P(n)$ to prove $P(n+1)$. This can make the job much easier in many cases.
Consider the following problem: prove that every integer $n \geq 1$ can be written as a sum of distinct powers of two. The base case $n = 1$ is pretty easy since $1 = 2^0$. Let's prove the induction step using strong induction. Let n be arbitrary, and suppose $P(1), P(2), \ldots, P(n)$ are all true. We want to prove that $P(n+1)$ is true. Let us look at the case when $n+1$ is odd. Using the inductive assumption we know $P(n)$ is true, i.e. n can be written as a sum of distinct powers of two: $n = 2^{a_1} + \ldots + 2^{a_k}$, for some k distinct powers $a_1, \ldots, a_k$. Note that 2^0 does not occur in the sum-of-distinct-powers-of-two expression for n since n is even (why?). Thus, we can write $n+1$ as $1+n = 2^0 + (2^{a_1} + \ldots + 2^{a_k})$. Now consider the case when $n+1$ is even. Unlike the odd case, in this case, 2^0 can occur in the sum-of-distinct-powers-of-two expression for n, and so we cannot simply add 2^0 to that expression. Instead, we will look at the expression for $(n+1)/2$ (since it is an integer). Because we are using strong induction, we know that $P((n+1)/2)$ is true, and thus we have a sum of powers of two representation for $(n+1)/2$. Say the representation is $(n+1)/2 = 2^{b_1} + \ldots + 2^{b_\ell}$, where the b_is are distinct

[1] The base case need not always be $n = 0$. It really depends on what statement you are trying to prove. For example, sometimes, the statement might only assert something about integers $n \geq 2$, in which case your base case will be $n = 2$.

numbers. But this means that $n+1 = 2^{b_1+1} + \ldots + 2^{b_\ell+1}$ (this is just multiplying both sides by 2 in the previous expression). This finishes the proof.

This finishes our review of some important 205 concepts. Be sure to practice and study a bit more on your own!

5 The sum rule

In counting, the goal is to find $|X|$ for some set X. Of course, if you knew X "explicitly" you could just "count" how many elements it has. However, in most situations, you only have an "implicit" description of X (and this will become clearer in the next lecture when we see tons of examples of counting problems), and this makes counting the number of elements in X challenging.

The first basic rule we have for counting is the *sum rule*: suppose A and B are disjoint sets, then

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

This commonsensical rule has far-reaching applications (as we shall see next time). When A and B are not disjoint, we know that $|A \cup B| = |A| + |B| - |A \cap B| \leq |A| + |B|$. The inequality $|A \cup B| \leq |A| + |B|$ is called the *union bound*, and we shall see powerful applications of it later on in the course.