Class 25: Counting

Schedule

Reminder for the schedule for the rest of the semester:

– **Problem Set 9**: due on Friday, 1 December at 6:29pm.
– **Problem Set omega;**: due on Monday, 4 December at 11:59pm. See the Problem Set omega; description for examples from previous students.
– **Final Exam**: Thursday, 7 December, 9am-noon (in the normal lecture room)

Examples

Today, we want to bre able to answer the following questions. The first two are already discussed in class, but we will study them more generally.

1. How many subsets does S have if $|S| = n$?
2. How many numbers are there that can be represented with (at most) n bits (in base 2) ?
3. How many (at most) 16-bit numbers with exactly 4 ones?
4. How many ways to choose 12 doughnuts from 5 varieties?

The first two have the same answers 2^n. In fact, because there is a bijection between the set of answers to problem 1 and problem 2, then we already knew that they have the same answers. More generally, all counting problems of today's class could be described as "what is the size of a set A?" We use the definitino of finite cardinality from Class 9, to study these questions. Namely, we try to find another set B whose cardinality is knwon, and that there is a bijection between A and B.

Why Counting?

Being able to count (exactly or even approximately) is important for many reasons, some of which are:

– Estimating the "cost" of an algorithm, this could be time, space, etc. This comes up when we try to analyze the "efficiency" of an algorithm.

– Estimating the "security" of a cryptographic algorithm. Basically, we would like to know how big is the "space of keys" from which the adversary has to "guess" the correct one.

– Counting is the fundamental to probability theory.

Counting Rules

Product Rule If $A_1, \ldots, A_n$ are finite sets, then the size of their cartesian product is

$$|A_1 \times \ldots \times A_n| = |A_1| \cdot |A_2| \ldots |A_n|$$

We previously saw this rule in Class 7, but we will use it more heavily today, and we will see some extensions of it.

Using the product rule, formally prove that the answer to the first two example problems are both 2^n. (Hint, let $S = \{a_1, \ldots, a_n\}$ and let $A_i = \{a_i\}$.)

Sum Rule. If $A_1, \ldots, A_n$ are finite *disjoint* sets, then the size of their *union* is

$$|A_1 \cup \ldots \cup A_n| = |A_1| + |A_2| \cdots + |A_n|.$$

The sum rule is even simpler than the product rule, but together with the product rule, theye become very powerful.

Using the product and sum rules, count now many passwords of 6 to 8 characters exist if the first character can be an english letter (upper or lower case) and the rest could also be a digit.

Generalized product rule Suppose S is a set containing length-k sequences like $(a_1, \ldots, a_k)$. If there are n_i possibilities for i'th entry a_i for any possible prefix $a_1, \ldots, a_{i-1}$, then $|S| = n_1 \cdot n_2 \ldots n_k$.

Using the generalizd product rule, prove that the number of permutations over any set $S = \{s_1, \ldots, s_n\}$ is $n!$. A permutation is simply a sequence $(a_1, \ldots, a_n)$ where each s_i appears in that sequence exactly once.

Division Rule. If $f : A \to B$ is a k to 1 (total surjective) function, and if A, B are finite sets then, $|A| = k \cdot |B|$.

Counting when order does not matter

The number of subsets of size k of $\{1, \ldots, n\}$ captures a counting problem in which the order of the k selected elements does not matter. This number is so important that has its own notation $\binom{n}{k}$.

Using the division rule, prove that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ #

 Creative Commons Attribution-Noncommercial-Share Alike 3.0