CPSC 202 Notes **Fall 2017**

Notes 1: December 12

Author: Kevin Truong *Scribes:*

Note: *Quick Reference on Probability Theory, CRT, Relations, Graphs, and Counting*

1.1 Probability Axioms

1.1.1 Axioms

Probability ranges from 0 to 1. Discrete probability deals with finite axioms. A triple is a set of outcomes (Ω, F, P). Kolmogrov has three axioms: 1.P(A) $\geq$ 1, 2. P(Ω) = 1, 3. Sum of disjoint proabilities is the summation of the individual probailities.

Examples of good probability problems:

- probability of choosing a bit is 1/2
- probability of choosing from a regualar die is 1/6
- probability of a roll of the dice in which order matters is 1/36
- number of n bit strings is 2^n and the number of strings with with exactly one 1 is n
- chossing 5 cards from a deck in which order does and does not matter is $\binom{n}{5}$ and $(n)_5$

If two probabilities are independent, the probability that both of them occur is P(A)P(B).

1.1.2 Inclusion - Exclusion Principle

$$Pr[A \cup B] = Pr[A] + Pr[B] - Pr[A \cap B] \tag{1.1}$$

1.1.3 Conditional Probability and Chain Rule

$$Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} Pr[A \cup B] = Pr[A|B]Pr[B] \tag{1.2}$$

1.1.4 Marginal Probability

$$Pr[A] = \sum_{i=1}^{n} Pr[A|B_i]Pr[B_i]. \tag{1.3}$$

1.1.5 Random Variables

A random variable X is a variable that takes on particular values randomly. This means that for each possible value x, there is an event [X = x] with some probability of occurring that corresponds to X (the random variable, usually written as an upper-case letter) taking on the value x (some fixed value).

If the random variables are independent:

$$Pr[X = x \wedge Y = y] = Pr[X = x]Pr[Y = y] \tag{1.4}$$

The expectation of a variable is the average value:

$$E[X] = \sum_x xPr[X = x] \tag{1.5}$$

The expectation operator is linear: this means that E [X + Y] = E [X] + E[Y] and E[aX] = aE[X] when a is a constant.

For products of random variables, the situation is more complicated. Here the rule is that E[XY] = E[X] E[Y] if X and Y are independent.

The conditional expectation:

$$E[X] = \sum_i E[X|A_i]Pr[A_i] \tag{1.6}$$

Useful expectation stuff to know:

- E[aX +bY|Z] = aE[X|Z] +bE[Y|Z]. This is the conditional expectation version of linearity of expectation
- E[X|X]=X
- If X and Y are independent, then E[Y|X] = E[Y].
- E [E [X |Y]] = E [X]

Expectation squared:

$$E[(X + Y)^2|X] = E[X^2|X] + 2E[XY|X] + E[Y^2|X] = X^2 + 2XE[Y] + E[Y^2] \tag{1.7}$$

1.1.6 Variance

$$E[X^2] - (E[X])^2 \tag{1.8}$$

$$Var[cX] = c^2Var[X] \tag{1.9}$$

$$\begin{aligned} Var[X + Y] &= E[(X + Y)^2](E[X + Y])^2 && (1.10)\\ &= Var[X] + Var[Y] + 2(E[XY]E[X]E[Y]). && (1.11) \end{aligned}$$

1.2 Chinese Remainder Theorem

1.2.1 Working Example of CRT

Find x such that

$$x \equiv 2 \; mod \; 3 \tag{1.12}$$

$$x \equiv 2 \; mod \; 4 \tag{1.13}$$

$$x \equiv 1 \; mod \; 5 \tag{1.14}$$

There exists a unique x such that $0 \leq x \leq 3 * 4 * 5$.

$$x = 5 * 4 + 3 * 5 * (3 * 2) + 3 * 4(3) \tag{1.15}$$

$$x = 196 \tag{1.16}$$
$$x = 26 \; mod \; 60 \tag{1.17}$$

1.2.2 Euler's Theorem

$$\phi(n) = \prod_{i=1}^{k} p_i^{e_i - 1} p_i - 1 \tag{1.18}$$

Example would be finding the $\phi(12)$:

$$\phi(12) = 2^2 * 3^1 \tag{1.19}$$
$$= 2^{2-1} * (2-1) * 3^{1-1} * (3-1) \tag{1.20}$$
$$= 4 \tag{1.21}$$

This means that there are 4 digits between 0 and 12 that are unique prime to 12

For the case which the gcd of a and m is 1:

$$a^{\phi(m)} = 1 \; mod \; m \tag{1.22}$$

For the case which m is prime, implies Little Fermat's Theorem:

$$a^{p-1} = 1 \; mod \; p \tag{1.23}$$

1.3 Relations

1.3.1 Representing relations

We can represent relations visually as graphs or matrices.

1.3.2 Operations on relations

Relations can be composed. Matrices can be composed and this is very similar to matrix multiplication. Relations can also have inverses

1.3.3 Classifying Relations

Relations must have these properties:

- reflexivity (aRa)
- antisymmetry (aRb and bRa) only if a = b
- symmetry (aRb and bRa)
- transitivity (aRb and bRc implies aRc)

1.3.4 Reflexivity

The equality relation is in a sense particularly reflexive: a relation R is reflexive if and only if it is a superset of =.

1.3.5 Symmetry

Another way to state symmetry is that R = R^{-1}.

1.3.6 Transitive

The set-theoretic form is that R is transitive if $R^2 \subset$ R, or in general if $R_n \subset$ R for all $n > 0$.

1.3.7 Equivalence Reations

An equivalence relation is a relation that is reflexive, symmetric, and transitive.

Transitivity gives rise to equivalence classes. Any equivalence relation $\sim$ on a set A gives rise to a set of equivalence classes, where the equivalence class of an element a is the set of all b such that a $\sim$ b.

We can partition a set based on the quivalence class.

Theorem 1.1 *Let $\sim$ be a relation on A. Then each of the following conditions implies the others:*

- $\sim$ is reflexive, symmetric, and transitive.
- There is a partition of A into disjoint equivalence classes A_i such that x $\sim$ y $\iff \exists\, ix \in A_i \wedge y \in A_i$.

1.3.8 Partial orders

A partial order is a relation $\leq$ that is reflexive, transitive, and antisymmetric. A strict partial order is a relation $<$ that is irreflexive (x $\nless$ x) and transitive.

A total order is a partial order in which any two elements are comparable. This means that, given x and y, either x $\leq$ y or y $\leq$ x. A poset (S, $\leq$) where is a total order is called totally ordered.

Examples of posets and total orders:

- $\leq$
- $\geq$

Examples of just posets:

- divisibility
- the product of two posets
- Let $\sum$ be some alphabet and consider the set$\sum = \sum * \cup \sum^1 \cup \sum^2 \ldots$ of all finite words drawn from $\sum$. Given two words x and y, let x $\leq$ y if x is a prefix of y. If there is some word z such that xz=y. Then $(\sum, \leq)$ is a poset.

1.3.9 Hasse Diagrams

A way of representing partial orders that omits edges from reflexivity and transitivity

1.3.10 Comparability and Lattices

Two elements are comparable if xRy or yRx. If they can not be compared in anyway, they are called imcomparable. In a Hasse diagram, the elements of the paths going up are all comparable. Sister nodes are not comparable because they are not on the same path.

Total orders are partial orders in which any two elements in the lattice can be compared. Any partial order can be "closed" to become a total order. All total orders are lattices

Lattices is defined by the fact that for any two points in the lattice, the two points have both a local max and min. The lattice must also have an absolute max and min.

Examples of lattices:

- total orders
- divisibility
- gcd

1.3.11 Well Orders

A well order is a particularly restricted kind of total order. A partial order is a well order if it is a total order and every nonempty subset S has a minimum element x.

An equivalent definition is that a total order is a well order if it contains no infinite descending chain, which is an infinite sequence $x_1 > x_2 > x_3 > \dots$

1.3.12 Closures

The **reflexive closure** of a relation R (whose domain and codomain are equal) is the smallest super-relation of R that is reflexive; it is obtained by adding (x, x) to R for all x in Rs domain, which we can write as $R^0 \cup R$ where R^0 is just the identity relation on the domain of R. $R = R_0 \cup R_1 \cup R_2 \dots$

The **symmetric closure** is the smallest symmetric super-relation of R; it is obtained by adding (y, x) to R whenever (x, y) is in R, or equivalently by taking $R \cup R^{-1}$.

The **transitive closure** is obtained by adding (x, z) to R whenever (x,y) and (y,z) are both in R for some yand continuing to do so until no new pairs of this form remain.8 The transitive closure can also be computed as $R+ = R_1 \cup R_2 \cup R_3 \dots$

One can do multiple closures at once. The goal of doing this is to make parti orders and equivalence relations. The only property that can not be closed is antisymmetry.

1.4 Counting

1.4.1 Combinatorics

Counting a set A using a bijection f : A $\rightarrow$ [n] gives its size $|A| = n$; this size is called the cardinality of n

For infinite sets, cardinality is a little more complicated. The basic idea is that we define $|A| = |B|$ if there is a bijection between them.

1.4.2 Inequalities

We write $|A| \leq |B|$ if there is an injection f : A $\rightarrow$ B, and similarly $|B| \leq |A|$ if there is an injection g : B $\rightarrow$ A. If both conditions hold, then there is a bijection between A and B, showing $|A| = |B|$.

Similarly, if we write $|A| \geq |B|$ to indicate that there is a surjection from A to B, then $|A| \geq |B|$ and $|B| \geq |A| \implies |A| = |B|$.

If A and B are finite sets with $A \cap B =$, then $|AB| = |A| + |B|$.

$$\cup_i^k A_i = |A_i|. \tag{1.24}$$

For infinite sets: $|A| + |B| = \max(|A|, |B|)$

1.4.3 Pigeonhole Principles

If there are n items to fit into b bins, there will be at least one bin that has ceiling n/b items

1.4.4 Subtraction, Multiplication, and exponeniation

$$|A \backslash B| = |A| - |A \cap B| \tag{1.25}$$

$$|A * B| = |A| * |B| \tag{1.26}$$

Given sets A and B,let A $\rightarrow$ B be the set of functions f:B $\rightarrow$ A. Then $|A^B| = |A|^{|B|}$.

1.4.5 Counting Injections

This gives us three tools for counting functions between sets:

- n^k counts the number of functions from a k-element set to an n-element set
- $(n)_k$ counts the number of injections from a k-element set to an n-element set
- n! counts the number of bijections between two n-element sets (or from an n-element set to itself).

1.4.6 Division

Sometimes we can compute the size of a set S by using it (as an unknown variable) to compute the size of another set T (as a function of $|S|$), and then using some other way to count T to find its size, finally solving for $|S|$. This is known as counting two ways and is surprisingly useful when it works. We will assume that all the sets we are dealing with are finite, so we can expect things like subtraction and division to work properly.

1.4.7 Binominal

$$\binom{n}{k} = \frac{n!}{((n-k)!k!} \tag{1.27}$$

1.4.8 Counting examples

Sometimes reducing to a previous case requires creativity. For example, suppose you win n identical cars on a game show and want to divide them among your k greedy relatives. Assuming that you dont care about fairness, how many ways are there to do this?

If its OK if some people dont get a car at all, then you can imagine putting n cars and k 1 dividers in a line, where relative 1 gets all the cars up to the first divider, relative 2 gets all the cars between the first and second dividers, and so forth up to relative k who gets all the cars after the (k 1)-th divider. Assume that each carand each dividertakes one parking space. Then you have n + k 1 parking spaces with k 1 dividers in them (and cars in the rest). There are exactly $\binom{n+k-1}{k}$ ways to do this.

Alternatively, suppose each relative demands at least 1 car. Then you can just hand out one car to each relative to start with, leaving n k cars to divide as in the previous case. There are (nk)+k1 = n1 k1 k1 ways to do this.

1.5 Binomial Coefficients

$$(x+y)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k y^{n-k} \tag{1.28}$$

$\binom{n}{k}$ is defined as $\frac{(n)_k}{k!}$, so negative numbers still work

1.5.1 Pascal's Triangle

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \tag{1.29}$$

1.5.2 Vandermonde's Identity

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} + \binom{n}{k} \tag{1.30}$$

1.5.3 Number of subsets

$$\sum_{0}^{k} \binom{n}{k} = 2^n \tag{1.31}$$

1.5.4 Negative Binomials

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k} \tag{1.32}$$

1.5.5 Generating functions

$$F(z) = \sum_{0}^{\infty} a_i z^i \tag{1.33}$$

Examples of good generating functions to know:

- $\frac{1}{1-z} = \sum_0^\infty z^i$
- $\frac{1}{(1-z)^2} = \sum_0^\infty i z^i$
- $\frac{1}{(1-z)^n} = \sum_0^\infty \binom{n+i-1}{i} z^i$
- $(1+z)^n = \sum_0^\infty \binom{n}{i} z^i$

1.5.6 Recurrence section

Generating Function in the form of a past or future value. A standard trick in this case is to multiply each of the ∀ i bits by z_n, sum over all n, and see what happens

1.5.7 Adding Generating Functions

Suppose C = A ∪ B and A and B are disjoint. Then the generating function for objects in C is F (z) + G(z).

Example: Suppose that A is the set of all strings of zero or more letters x, where the weight of a string is just its length. Then F (z) = 1/(1 - z), since there is exactly one string of each length and the coefficient ai on each zi is always 1. Suppose that B is the set of all strings of zero or more letters y and/or z, so that G(z) = 1/(1-2z) (since there are now 2^i choices of length-i strings). The set C of strings that are either (a) all xs or (b) made up of ys, zs, or both, has generating function F (z) + G(z) = 1/(1 - z) + 1/(1 - 2z).

1.5.8 Multiplying Generating Functions

$$F(z)G(z) = \sum_{i=0}^{\infty} \sum_{j=0}^{i} a_j b_{j-i} z^i \tag{1.34}$$

1.5.9 Repetition

$$H = 1 + F + F2 + F3 + \ldots = \frac{1}{1-F} \tag{1.35}$$

Example: the regular taylor series

$$1 + x^2 + x^3 \ldots \tag{1.36}$$

(0|11)∗ Let A = {0, 11}, and let C be the set of all sequences of zeros and ones where ones occur only in even-length runs. Then the generating function for A is $z + z^2$ and the generating function for C is $\frac{1}{(1-z-z^2)}$. We can extract exact coefficients from this generating function using the techniques below.

1.5.10 Pointing

$$H(z) = z^n \frac{d^n}{dz^n} F(z) \tag{1.37}$$

Count the number of finite sequences of zeros and ones where exactly two digits are underlined

1.5.11 Composition of Generating Functions

$$F(G(z)) = \sum_{0}^{\infty} a_k (G(z))^k \tag{1.38}$$

1.5.12 Recovering coefficients from generating functions

- Recognize the generating function from a table of known generating functions, or as a simple combination of such known generating functions. This doesnt work very often but it is possible to get lucky.
- To find the k-th coefficient of F(z), compute the k-th derivative d^k/dz^k F(z) and divide by k! to shift a_k to the z_0 term. Then substitute 0 for z.
- If the generating function is of the form 1/Q(z), where Q is a polynomial with $Q(0) \neq 0$, then it is generally possible to expand the generating function out as a sum of terms of the form $\frac{Pc}{(1-z/c)}$ where c is a root of Q (a value such that Q(c) = 0).

1.5.13 Patrial Fraction Decomposition

$$\frac{1}{(1-az)(1-bz)} = \frac{A}{1-az} + \frac{B}{1-bz} \tag{1.39}$$

$$A(1-az) + B(1-bz) = 1 \tag{1.40}$$

$$A + B = 1 \tag{1.41}$$

$$-A - B = 0 \tag{1.42}$$

1.6 Graphs

1.7 Linear Algebra