Math 311W (Discrete Math) Midterm 2 Review

Spencer Martz

March 22, 2024

2.1 Set Theory

A set is a collection of objects or, called "elements" or "members". The contains symbol $\in$ is used to denote if an object is an element of a set, and the subset symbol $\subseteq$ is used to denote if one set is contained within another.

- $x \in X$ means x is an element of X, and
- $x \notin X$ means x is not an element of X
- $X \subseteq Y$ means X is contained within Y (and may be equal), that is, $\forall x \in X, x \in Y$
- $X \subset Y$ means is X is contained within (as above), but is not equal to Y.

Some special objects are:

- the empty set $\varnothing : \{\}$, the set with no elements and
- U, the universal "set", or collection of all objects currently being considered, and
- $P(X)$, the power set of X, or set of all subsets of X.

Sets are usually defiend either by listing their elements or decribing some rule which determines if an object is an element. The order of elements does not matter.

The Algebra of Sets, $P(X)$

We say that the powerset $P(X)$ of X is an algebra of sets, which has certain operations which are permitted on it's elements

- Union $X \cup Y$: The set of elements in X or in Y – OR
- Intersection $X \cap Y$: The set of elements in both X and Y – AND
- Complement X^c: The set of elements which are not in X (and are in U)
- Relative complement: $X \backslash Y$: The set of elements which are in X and not in Y

Note that the powerset has 2^n elements, where n is the size of X. This is becuase to form a subset of X, we iterate over each element of X and choose whether or not to include it, and every different sequence of choices produces a different subset. Now for each element, there are two choices (whether or not it is in the subset), so the total number of choices (and thus subsets) is $2 * 2 * 2 \ldots$ n times, or 2^n.

Two sets X, Y are said to be equal if they have exactly the same elements. To show this (in a proof), one shows first that

1. that each elements of X is in Y, and each element of Y is in X, and thereby
   $(\forall x \in X, x \in Y \text{ and } \forall y \in Y, y \in X)$
2. $X \subseteq Y$ and $Y \subseteq X$, which implies that
3. $X = Y$

The following identites are proven by this method, and basic reasoning about the propeties of the operations.(Venn diagrams are usually of great assistance in this) None of them besides De'morgans laws are paticularly difficult.

Theorem 2.1.1: Properties of Set Operations

$X \cup X = X$
$X \cap X = X$ Idemoptence

$X \cup Y = Y \cup X$
$X \cap Y = Y \cap X$ Commutatitivity

$X \cup (Y \cup Z) = (X \cup Y) \cup Z$
$X \cap (Y \cap Z) = (X \cap Y) \cap Z$ Associativity

$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$
$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ Distributivity

$X \cap X^c = \varnothing$
$X \cup X = U$
$(X^c)^c = X$ Properties of Complement

$X \cup \varnothing = X$
$X \cap \varnothing = \varnothing$
$X \cup U = U$
$X \cap U = X$ Propeties of Empty and Universal set

$X \cap (Y \cup X) = X$
$X \cup (Y \cap X) = X$ Absorbtion Laws

$(X \cup Y)^c = X^c \cap Y^c$
$(X \cap Y)^c = X^c \cup Y^c$ De'morgans Laws

Proof of (the first of) De'morgans laws: We must show that:

$$(X \cup Y)^c \subseteq X^c \cap Y^c, \text{ and } Y^c \cap X^c \subseteq (X \cup Y)^c \tag{1}$$

and thereby $(X \cup Y)^c = X^c \cap Y^c$

To begin, consider an element $x \in (X \cup Y)^c$. Then $x \notin X \cup Y$, so x is not in X or in Y. This means $x \in Y^c$ and $x \in X^c$, so $x \in X^c \cap Y^c$:

Thus any element $x \in (X \cup Y)^c$ is also in $X^c \cap Y^c$, or $(X \cup Y)^c \subseteq X^c \cap Y^c$.

Now conversely, consider an element $x \in X^c \cap Y^c$. So x is in X^c and Y^c, which means x is not in X, and x is not in Y, so x is not in $X \cup Y$, and $x \in (X \cup Y)^c$:

Thus any element $x \in X^c \cap Y^c$ is also in $(X \cup Y)^c$, or $X^c \cap Y^c \subseteq (X \cup Y)^c$

Together then, since $X^c \cap Y^c \subseteq (X \cup Y)^c$ and $(X \cup Y)^c \subseteq X^c \cap Y^c$, $(X \cup Y)^c = X^c \cap Y^c$ □

Cartesian Product, $X \times Y$

The cartesian product of two sets, X and Y, is the set of ordered pairs, with the first element from X, and the second element from Y, that is,

$$X \times Y = \{(x, y) | x \in X \text{ and } y \in Y\} \tag{2}$$

For example, $\{0, 1, 2\} \times \{3, 4, 5\} = \{(0, 3), (0, 4), (0, 5), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$. These products are often useful to encode geometric objects or regions- a rectangle is a carteisan product of two intervals. Often times repeated cartersian products are denoted with power notations, so $R \times R = R^2$ (the (cartesian) plane).

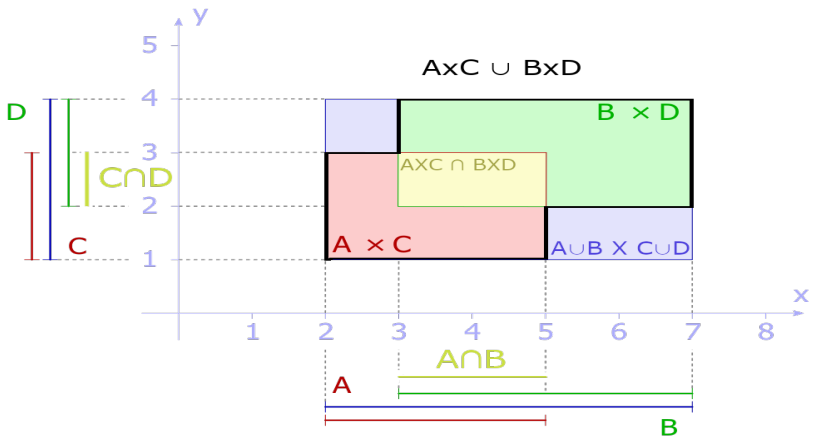
It is a trivial and fundamental fact that the size of $X \times Y$ is that of X times Y, or $|X \times Y| = |X| \cdot |Y|$. Less trivially, we have:

$$(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$$

however,

$$(A \times C) \cup (B \times D) \neq (A \cup B) \times (C \cup D)$$

,



Cardinality, $|X|$

Cardinality, denoted $|X|$ for a set X, is a measure of the size of a set. For finite sets, it is simply the number of (distinct) elements in the set. We say (paticuarly for infinite sets) that $|X| = |Y|$ iff there is some bijection from X to Y. As an example, take the positive integers $\mathbb{P}$ and the integers $\mathbb{Z}$. Since we may (uniquely) assign each odd element (e.g. $\{1, 3, 5, \dots\}$) to $\mathbb{Z}_+$, and each even element $\{2,\ 4,\ 6,\ \dots\}$ to $\mathbb{Z}_-$, it follows that we have a bijection from $\mathbb{P} \to \mathbb{Z}$, and thus $|\mathbb{P}| = |\mathbb{Z}|$

Theorem 2.1.2: Cardinality of Disjoint Sets

Two sets X and Y are said to be disjoint if they do not share any element in common, that is $X \cap Y = \varnothing$. In that case, we have:

$$|X + Y| = |X| + |Y| \tag{3}$$

Proof: Suppose $|X| = m, |Y| = n$, so there are bijections $f : X \to \{1, 2, 3, \dots m\}$ and $g : Y \to \{1, 2, 3, \dots n\}$. Consider

$$h : X \cup Y \to \{1, \dots m + n\} = \begin{cases} f(x) \text{ for } x \in X \\ g(x) + n \text{ for } x \in Y \end{cases}$$

Now since $X \cap Y$ is empty, h(x) is well defined (in that is does not map one input to more than one output), and additionally since f and g are both bijections, h is a bijection, in paticular to the set $\{1, 2, 3, \dots n, n + 1, \dots m + n\}$, which implies $|X \cup Y| = m + n = |X| + |Y|$, proving the theorem. □

Corollary 2.1.2: A more general (and useful) cardinality rule

For any finite sets X and Y,

$$|X + Y| = |X \cup Y| + |X \cap Y| \tag{4}$$

Proof: Consider the sets $X \cap Y$ and $X \backslash (X \cap Y)$, and observe they are disjoint with a union X. So by theorem 2.1.2,

$$|X \cap Y + X \backslash (X \cap Y)| = |X \cap Y| + |X \backslash (X \cap Y)| = |X| \implies |X \backslash (X \cap Y)| = |X| - |X \cap Y|$$

Now consider $X \backslash (X \cap Y) = X \cap Y^c$ and Y, also disjoint and with a union $X \cup Y$:

$$Y \cup (X \cap Y^c) = (Y \cup X) \cap (Y \cup Y^c) = (Y \cup X) \cap U = X \cup Y$$

Finally, by theorem 2.1.2,

$$\begin{aligned} |Y + X \backslash (X \cap Y)| &= |Y| + |X \backslash (X \cap Y)| = |X \cup Y| \\ |Y| + |X| - |X \cap Y| &= |X \cup Y| \\ |X| + |Y| &= |X \cup Y| + |X \cap Y| \end{aligned}$$

□

2.2 Functions

Function A function from the set X to the set Y is an assignment or rule which assigns each element x in X to some (single) element y in Y, such that f(x) = y.

We say that X is the domain, and Y is the codomain.

Two functions f and g are equal if their domains and codomains are equal, and $\forall x \in X, f(x) = g(x)$

Image and Graph The image of a function, denoted $im(f)$, is the set of all x in X under f(x): $\{f(x) \mid x \in X\}$, and is a subset of Y.

The graph of a function, denoted $gr(f)$, is the set of ordered pairs of elements of x and their image: $\{(x, f(x)) \mid x \in X\}$. Another more rigourous definition of a function follows:

A function is a subset of $X \times Y$ s.t. $\forall x \in X, \exists$ a unique $y \in Y$ s.t. $(x, y) \in gr(f)$

Injection A function is injective if, for all $x \in X$, there is a unique element $y \in Y$ s.t $f(x) = y$, or alternatively, $f(x) = f(x') \iff x = x'$

Surjection A function is surjective, or "onto" if, $\forall y \in Y, \exists x \in X$ s.t. $f(x) = Y$, or alternatively, $im(f) = Y$

Bijection A function is bijective, or "one-to-one" if it is injective and surjective, that is, $\forall y \in Y, \exists$ a unique $x \in X$ s.t. $f(x) = y$

Identity function id_x, the function which maps each element in X to itself, $x \mapsto x$.
For $f : X \to Y$ We have: $f(id_x) = f,$ and $id_y(f) = f$
The identity function is a bijection.

Inverse function For $f : X \to Y$, the inverse of f, $f^{-1} : Y \to X$ is the function which reverses the effect of f, or, $ff^{-1} = id_y,\ f^{-1}f = id_x$
The inverse of a function exists iff it is a bijection.

Compositions of Functions

Let $f : X \to Y, g : Y \to Z$ be functions, define gf to be the "composition of f and (then) g", $g(f(x))$. For composition of the same function, often power notiation is used, eg. $ff = f^2$

Theorem 2.2.1: Associativity of Compososition of Functions

For functions $f : X \to Y, g : Y \to Z, h : Z \to W$, hg(f) = h(gf). The proof is trivial, simply consider the possible paths an element may take.

Theorem 2.2.2: Uniqueness of the Inverse Function

If a function $f : X \to Y$ has an inverse, it is unique.

Proof: Suppose both g and h are inverses of f, so $hf = gf = id_x, fg = fh = id_y$.
Consider $(gf)h = (id_x)h = h,$ and $g(fh) = g(id_y) = g$ Then by theorem 2.2.1, $(gf)h = g(fh) \implies h = g$ □

Theorem 2.2.3: A function $f : X \to Y$ has an inverse $\iff$ it is a bijection

Proof: ($\Rightarrow$) Suppose f^{-1} exists, and consider $f(x_1) = f(x_2)$. We have:

$$f(x_1) = f(x_2) \implies f^{-1}f(x_1) = f^{-1}f(x_2) \implies id_x(x_1) = id_x(x_2) \implies x_1 = x_2$$

So f is injective.
Now, consider some $y \in Y$ and consider $ff^{-1}(y) = id_y(y) = y$
We see y may be written in the form $f(x)$, where $x = f^{-1}(y) \in X$,
which implies f is surjective, so together with injectivity, f is bijective.

($\Leftarrow$) Now suppose f is a bijection, and define $f^{-1} : Y \to X$, where $f^{-1}(y) = x \iff f(x) = y$ Since F is injective, f^{-1} is "well-defined" (does not map one inpute to multiple output), and since f is surjective, each y in Y maps to atleast one element $x \in X$. It follows that $f^{-1}f = id_x$ and $ff^{-1} = id_y$, so f^{-1} is the inverse of f. $\square$

2.3 Relations

Defintion and Special Examples

Relations are a more generalized idea of a function which describes certain cases which functions do not allows, paticulary, it allows multiple inputs to "relate" to multiple outputs. A relation R from the sets X to Y is a subset of $X \times Y$; $R \subseteq X \times Y$. Often, instead of $(x, y) \in R$, xRy is used to denote that x is related to y. In the case that X=Y, (that the relation is between the same sets), then we say R is a relation on X.

Many common mathematical objects are relations. $=, \geq, \leq, <, >, a|b, \equiv, \ldots$. Below are some imporant examples of relations.

Empty relation $\varnothing \subseteq X$, such that no element $x \in X$ is related to $y \in Y$

Identity relation $R = \{(x, x)|x \in X\}$, xRx if x = x

Dual or Complement relation For some relation R on X to Y,
define $R^c = (X \times Y) \backslash R$ as the complement (or dual) relation of R.

Reverse relation For some relation R on X to Y,
define $R^{rev} = \{(y, x)|(x, y) \in R\}$ as the reverse relation of R.

Properties of Relations (on a set)

Certain properties hold for relations on a set X (not on X to Y). We say R is:

Reflexive if, for all x in X, x is related to itself: $\forall x \in X, xRx$

Symmetric if x is related to y, then y is related to x: $\forall x, y \in X, xRy \iff yRx$

Weakly antisymmetric if, x related to y and y related to x implies that x = y:
xRy and $yRx \implies x = y$

Antisymmetric If xRy and yRx does not hold for any x and y: $xRy \implies y \not{R} x$

Transitive if, $\forall x, y, z \in X, xRy$ and $yRz \implies xRz$

To prove a relation has a certain property, one demonstrates that the property holds for all X. Here we will show that the (congrunce) relation

$$xRy \text{ if } n|x - y, \text{ that is, } x \equiv y \mod n \tag{5}$$

is reflexive, symmetric, and transitive.

- First we consider reflexivity: xRx holds $\forall x \in X$ since, $n|[0 = (x - x)]$ or $x \equiv x \mod n$ is true for all x, so R is reflexive.
- Next we consider if R is symmetric: suppose xRy holds, that is $n|x - y$.
  Then $nk = x - y$ f.s. $k \in Z$, and $n(-k) = y - x \implies n|y - x$, so yRx and R is symmetric.
- Lastly we show that R is transitive: suppose that xRy holds, that is $n|x - y,\ n|y - z$.
  Then $nk = x - y,\ np = y - z,\ n(k + p) = x - y + (y - z) = x - z$,
  so $n|x - z$, xRz and R is transitive.

Special Cases of Relations

1. Partial Ordering

- A partial ordering on X is a relation that is: reflexive, weakly antisymetric, and transitive.

  Examples include $\geq, \leq,$ and $A|B$.

- A strict partial ordering on X is a relation that is: antisymmetric and transitive.

  Examples include $< and >$.

- Additionally, for a strict partial ordering, x is an immediate successor of y (and y an immediate predessor of x) if xRy, and $\nexists z \in X$ s.t. xRz and zRy

2. Equivalence Relations

A relation on X is an equivalence relation if R is reflexive, symmetric, and transitive. In that case it may be denoted with E. Examples include: equality (=), congruence mod n ($\equiv$) (this was shown above), and matrix similarity.

Partitions and Equivlance Relations

Let X be any set. A partition P of X is a collection of non-empty subsets of X, $\{X_i | i \in I \subseteq Z\}$ which obeys two proprties:

1. P is disjoint, meaning $X_i \cap X_j = \varnothing \forall i \neq j$
2. P is covering, meaning $\forall x \in X, x \in X_i$ f.s. $i \in I$

Theorem 2.3.1: Partitions $\iff$ Equivalence Relations

- Given $P = \{X_i | i \in I\}$ is a partition of X. Then the relation xRy if x and y are in X_i is an equivalence relation
- Conversely, given an equivlance relation E, there is a partition on X with "blocks" X_i formed by the (distinct) equivalence classes of E; $[x]_E = \{y \in X | yEx\}$

Proof:

1. Given $\{X_i | i \in I\} = P$ is a partition on X, clearly the relation R described above is reflexive and symmetric. For transitivity, suppose we have xRy and yRz, so $x, y \in X_i, y, z \in X_j, \implies y \in X_i \cap X_j$. But since P is a partion, this implies $i = j$, and thus $x, y, z \in X_i$, and xRz holds.

2. Now given E, an equivilance relation on the set X, and the equivlance classes $[x] = [x]_E = y \in X | yEx$, then the unique sets of this kind form a partition on X. First we show that $b \in [a] \implies [b] = [a]$, and disjointedness will soon follow. Suppose we have $b \in [a]$ and consider some $c \in [a]$, we must show it is in [b]. Since $bEa \implies aEb$ by symmetry, and $cEa, aEb \implies cEb, c \in [b]$. Thus $[a] \subseteq [b]$. Conversly consider some $d \in [b]$ and similarly obervse: $dEb, bEa \implies dEa$ (by transitivity), thus $[b] \subseteq [a]$ and so $[a] = [b]$. Now we show P is disjoint and covering:

   Disjoint: suppose $c \in [a],$ and $c \in [b]$, then by the above:
   $[c] = [a], [c] = [b], \implies [b] = [a]$

   Covering: For all $a \in X$, a will be in some set of the form [x], namely [a].
   Thus P is disjoint, covering, and therefore defines a partition on X. $\square$

1.5 Linear Congruences

A linear congruence is an "equation" of the form

$$ax \equiv b \mod n \tag{6}$$

where a, b and n are fixed and x is a variable to solved for. In congruence classes the equation may be expressed:

$$[a]_n x = [b]_n \tag{7}$$

Theorem 1.5.1: Solvability of a system of linear congruences

1. The linear congruence $ax \equiv b \mod n$ has solutions if and only if the gcd of a and n, $d = (a, n)$ divides b.
2. In that case, the congruence has d unique solutions upto equivalence mod n, and each of these solutions are congruent mod $\frac{n}{d}$

Proof:

1. ($\Rightarrow$) Suppose that there is a solution to the congruence c, so $ac \equiv b \mod n$. Then $n|b - ac, nk = b - ac, b = nk - ac$, and observe that $d = (a, n)$ divides both nk and ac, and so d divides b.

1. ($\Leftarrow$) Now suppose d=(a,n) divides b, so cd=b. Now by bezout's identity, we have $d = sa + tn$ for $s, n \in Z$. Multiplying throughout by c yeilds

   $$cd = csa + ctn \implies b = csa + ctn \implies csa \equiv b \mod n$$

   so the congrunce has a solution, namely (cs).

2. Suppose we have a solution c. Then by the above $d = (a, n)|b$, and so we may divide the congruence throughout by D to yield:

   $$\frac{a}{d}c \equiv \frac{b}{d} \mod \frac{n}{d} \tag{8}$$

   So any solution of the original congruence is also a solution of the above, and conversely (by multiplying by d) the congrunce class of c mod $\frac{n}{d}$ is a soltuion of the original congruence. As such, for some solution c we have $[c]_{\frac{n}{d}} = \{c, c + \frac{n}{d}, c + \frac{2n}{d}, \dots\}$ are also solutions.

   Observe that $c + d(n/d) = c + n \equiv c \mod n$, and simiarly, $c + (d + 1)(n/d) \equiv c + (n/d)$, so there are unique sols for $0 \leq k \leq d - 1$, or d unique solutions.

This yeilds the following algorithim for solving linear congrungruences:

1. Determine $d = (a, n)$ and check if it divides b.
2. If not, stop. If so, there are d unique solutions. Now divide the congruence throughout, yielding:

   $$(a/d)x = (b/d) mod (n/d) \tag{9}$$

3. Find solutions to this congruence, of which there will be one since $a/d, n/d$ are coprime (their greatest common factor was divided).

   either by inspection, or by determining the inverse of a/d, call it e

4. Every solution to this congruence will be one of the original congruence, paticualrly of the form $[be/d]_{n/d}$, of which there are d unique solutions upto congruence mod n.

Theorem 1.5.2: Chinese Remainder Theorem

The system of congrunces:

$$x \equiv a \mod m$$
$$x \equiv b \mod n$$

has a solution if any only if m and n are coprime, that is $(m, n) = 1$. In that case the solution is unique up to congrunce mod mn.

Proof: Since $(m, n) = 1$, we have $sm + tn = 1$ for some $s, t \in Z$. Define

$$c = bsm + ant \tag{10}$$

and observe since $nt \equiv 1 \mod m$, $c \equiv ant \mod m \implies c \equiv a \mod m$, similarly $c \equiv b \mod n$ and thus c is a solution to the system of congrunences.

Now we show that the solution is unique upto congrunce mod n. Suppose there is a another solution d, so $d \equiv a \mod m$ and $d \equiv b \mod n$

Then we have that $c - d \equiv a - a \equiv 0 \mod m$, and $c - d \equiv b - b \equiv 0 \mod n$,
so $c \equiv d \mod n, c \equiv d \mod n$, $n|c - d, m|c - d$.

Now by theorem 1.1.6(ii), for a, b coprime, if $a|c$ and $b|c$, then $ab|c$. Taking $m = a, n = b, c - d = c$ we see that $mn|c - d$, and thus $c \equiv d \mod mn$ □

This yeilds the following algorithim for solving systems of linear congruences:

1. Check if m and n are coprime
2. If not, stop. If so there is a unique solution (upto congruence mod mn)
3. In that case, construct the solution $c = asn + btm$ (note, m and n "swap over"), and observe it is a solution to both congruences.

Non-linear congruences