CS1231S Pointers

Jia Cheng

September 2020

1 Definitions and Useful tidbits

$$\begin{aligned} &\mathbb{N} = \{0, 1, 2, \dots\} \\ \text{Primes from 1-100 } &:2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \\ &31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 \end{aligned}$$

2 Predicate Logic

2.1 Use of words

Remember to use **universal** modus ponens (as well as other argument forms) instead of modus ponens when necessary.

2.2 Uniqueness quantification

$$\exists! x\, P(x) \tag{1}$$

$$\exists x (P(x) \wedge \sim \exists y (P(y) \wedge y \neq x)) \tag{2}$$

$$\exists x (P(x) \wedge \forall y (P(y) \rightarrow y = x)) \tag{3}$$

$$\exists x\, P(x) \wedge \forall y \forall z (P(y) \wedge P(z) \rightarrow y = z) \tag{4}$$

$$\exists x \forall y (P(y) \leftrightarrow y = x) \tag{5}$$

Equation (4) is important because it splits the uniqueness quantification into 2 parts, existence and uniqueness.

CS1231S 2018 Midterms Q16c

Write a logical statement to mean “a cell cannot contain two digits”.

A subtlety here is that we are only required to state uniqueness, not existence. This is where equation (4) above becomes useful.

2.3 Identities

See Wikipedia: First-order logic - Provable identities
Also see prenex normal form

Negation

$$\begin{aligned} \sim \forall x\, P(x) &\equiv \exists x \ \sim P(x) \\ \sim \exists x\, P(x) &\equiv \forall x \ \sim P(x) \end{aligned}$$

Change of order

$$\begin{aligned} \forall x \forall y\, P(x,y) &\equiv \forall y \forall x\, P(x,y) \\ \exists x \exists y\, P(x,y) &\equiv \exists y \exists x\, P(x,y) \end{aligned}$$

Distributivity

$$\begin{aligned} \forall x\, (P(x) \wedge Q(x)) &\equiv \forall x\, P(x) \wedge \forall y\, Q(y) \\ \exists x\, (P(x) \vee Q(x)) &\equiv \exists x\, P(x) \vee \exists y\, Q(y) \end{aligned}$$

Conjuction and disjunction

$$\begin{aligned} P \wedge \exists x\, Q(x) &\equiv \exists x\, (P \wedge Q(x)) \\ P \vee \forall x\, Q(x) &\equiv \forall x\, (P \vee Q(x)) \end{aligned}$$

Conjunction and disjuncion
with additional condition that domain of x is non-empty

$$\begin{aligned} P \wedge \forall x\, Q(x) &\equiv \forall x\, (P \wedge Q(x)) \\ P \vee \exists x\, Q(x) &\equiv \exists x\, (P \vee Q(x)) \end{aligned}$$

3 Sets

3.1 Set membership

Given a set $S = \{x \in U | P(x)\}$ for some predicate $P(x)$.

$$\forall x \in U, (x \in S \iff P(x))$$

Hence to prove set equality between S and another set T, we can try to show

$$\forall x \in U, (x \in T \iff P(x))$$

Furthermore, given 2 sets $S = \{x \in U | P(x)\}$ and $T = \{x \in U | Q(x)\}$ for some predicates $P(x), Q(x)$, it suffices to show that

$$\forall x \in U, (P(x) \iff Q(x))$$

3.2 Set difference law

We know that $A - B = A \cap \overline{B}$. Then

$$\begin{aligned} A \cap B &= A \cap \overline{\overline{B}} && \text{Double complement law} \\ &= A - \overline{B} && \text{Set difference law} \end{aligned}$$

4 Functions

4.1 Definitions

4.1.1 Function equality

$$\begin{aligned}&\text{Suppose } f : A \to B \text{ and } g : C \to D\\ &\text{Then } f = g \iff (A = C) \land (B = D) \land (\forall x \in A,\ f(x) = g(x))\end{aligned}$$

4.1.2 Function composition

Let $f : A \to B$ and $g : C \to D$.
For $g \circ f$ to be well-defined, we must have $B = C$. i.e. codomain of f = domain of g.

4.1.3 Bijectivity

$$\begin{aligned}&\text{Suppose } f : A \to B \text{ is a bijection}\\ &\text{Then, } \forall y \in B, \exists! x \in A, (y = f(x))\end{aligned}$$

4.1.4 Checking for bijectivity

Given a function $f : A \to B$, there are 2 ways to check if f is bijective.

1. Show separately that f is injective and surjective.
2. Define a function $g : B \to A$, and show that $g = f^{-1}$, i.e.

$$\forall x \in A, \forall y \in B, (y = f(x) \iff x = g(y))$$

4.2 Floors and Ceilings

$$\begin{aligned}n \le x &\iff n \le \lfloor x \rfloor\\ n < x &\iff n < \lceil x \rceil\\ x \le n &\iff \lceil x \rceil \le n\\ x < n &\iff \lfloor x \rfloor < n\end{aligned}$$

The proof of the above is based on the below property of floor and ceiling, that is,

$$\begin{aligned}\lfloor x \rfloor &= \max\{k \in \mathbb{Z} \mid k \le x\}\\ \lceil x \rceil &= \min\{k \in \mathbb{Z} \mid k \ge x\}\end{aligned}$$

As we have already proven the existence and uniqueness of $\lfloor x \rfloor$, where $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$, we can easily use this inequality to show that if there exists $y \in \mathbb{Z}$ such that $\lfloor x \rfloor < y$, then $x < \lfloor x \rfloor + 1 \le y$. This shows the maximality of $\lfloor x \rfloor$ in the set $\{k \in \mathbb{Z} \mid k \le x\}$.

4.3 Other Lemmas

1. For all sets A, B, functions $f : A \to B$, and $X, X' \subseteq A$, we have $f(X \cup X') = f(X) \cup f(X')$.

Proof:
Suppose $y \in f(X \cup X')$.

Then $y = f(x)$ for some $x \in X \vee x \in X'$.
If $x \in X$, then $y = f(x) \in f(X)$.
If $x \in X'$, then $y = f(x) \in f(X')$.
Hence $y = f(x) \in f(X) \cup f(X')$.
Hence $f(X \cup X') \cup f(X) \cup f(X')$.

Suppose $y \in f(X) \cup f(X')$.
Then $y \in f(X) \vee y \in f(X')$. Let $y = f(x)$ for some $x \in A$.
If $y \in f(X)$, then $x \in X$.
If $y \in f(X')$, then $x \in X'$.
Either way, $x \in X \cup X'$.
Hence $y = f(x) \in f(X \cup X')$.
Hence $f(X) \cup f(X') \subseteq f(X \cup X')$.

2. For all sets A, B, **injective** functions $f : A \to B$, and $X, X' \subseteq A$, we have $f(X \cap X') = f(X) \cap f(X')$.

Proof:
Suppose $y \in f(X \cap X')$.
Then $y = f(x)$ for some $x \in X \cap X'$.
Then $x \in X \wedge x \in X'$.
Then $y = f(x) \in f(X) \wedge y = f(x) \in f(X')$.
Hence $y \in f(X) \cap f(X')$.
Hence $f(X \cap X') \subseteq f(X) \cap f(X')$.

Suppose $y \in f(X) \cap f(X')$.
Then $y = f(x_1)$ for some $x_1 \in X$ and $y = f(x_2)$ for some $x_2 \in X'$.
By injectivity of f, we know that $x_1 = x_2 = x$ for some $x \in X \cap X'$.
Hence $y = f(x) \in f(X \cap X')$.
Hence $f(X) \cap f(X') \subseteq f(X \cap X')$.

3. For all functions $f : A \to B$, $X \subseteq A$, $Y \subseteq B$, we have:

$$X \subseteq f^{-1}(f(X))$$
$$f(f^{-1}(Y)) \subseteq Y$$

If f is injective, then we also have $f^{-1}(f(X)) \subseteq X$, and as a consequence, $X = f^{-1}(f(X))$.
If f is surjective, then we also have $Y \subseteq f(f^{-1}(Y))$, and as a consequence, $f(f^{-1}(Y)) = Y$.

4.4 Mistakes

Midterm 2019 Q9

For all functions $f : \mathbb{R} \to \mathbb{R}$, f is surjective if and only if $f^{-1}(X) \neq \emptyset$ for all $X \in \mathcal{P}(\mathbb{R})$.

While this seems to be correct, note that the empty set $\emptyset \in \mathcal{P}(\mathbb{R})$, and we would obviously have $f(\emptyset) = \emptyset$.

5 Mathematical induction

5.1 Strong induction

Prove property $P(n)$ for $n \in \mathbb{Z}_{\geq m}$

Base cases: $P(m), P(m+1), \ldots, P(m+\lambda)$

2 ways to write induction hypothesis
Suppose $P(m), \ldots, P(k+\lambda)$ for some $k \in \mathbb{Z}_{\geq m}$. Then we wish to prove $P(k+\lambda+1)$ true.
Suppose $P(m), \ldots, P(k)$ for some $k \in \mathbb{Z}_{\geq m+\lambda}$. Then we wish to prove $P(k+1)$ true..

5.2 Well ordering principle

1. Extend the well ordering principle to any lower-bounded set of integers.

Let S be a non-empty set of integers bounded below by α, i.e. $\alpha \leq x \forall x \in S$. Define the cartesian sum of 2 sets S_1, S_2 as $S_1 + S_2 = \{x + y \mid x \in S_1,\, y \in S_2\}$.
Consider $S - \alpha = S + \{-\alpha\} = \{x - \alpha \mid x \in S\}$. Then it is clear that $S - \alpha \subseteq \mathbb{Z}_{\geq 0}$ and that this set is non-empty.
By the well-ordering principle, there exists some element $y_0 \in S - \alpha$ such that $y_0 \leq y \forall y \in S - \alpha$. By definition of $S - \alpha$, $y_0 = x_0 - \alpha$ for some $x_0 \in S$. We claim that this x_0 is the minimal element of S. To prove this, suppose x is any element of S. Then $x - \alpha \in S - \alpha$, hence $x_0 - \alpha \leq x - \alpha$, which implies $x_0 \leq x$. And we are done.

2. A symmetrical statement of the well-ordering principle. An upper bounded set of integers has a maximal element.

3. Using 1 and 2, we have the following theorem: For any set of integers bounded from both sides, there exists a minimum and maximum element.

We will the above to prove the following statement: For any positive integer x, there exists $\lambda \in \mathbb{Z}_{\geq 0}$ such that $2^{\lambda} \leq x \leq 2^{\lambda+1}$.
Let $S_1 = \{\lambda \in \mathbb{Z}_{\geq 0} \mid 2^{\lambda} \leq x\}, S_2 = \{\lambda \in \mathbb{Z}_{\geq 0} \mid 2^{\lambda} > x\}$.
It is trivial to see that $2^0 \leq x \leq 2^x$. This implies that S_1 is bounded above by x and S_2 is bounded below by 0.
Hence there exists a maximal element $\lambda_1 \in S_1$ and a minimal element $\lambda_2 \in S_2$. And we have $2^{\lambda_1} \leq x < 2^{\lambda_2}$. It now suffices to show that $\lambda_2 = \lambda_1 + 1$.
This can be easily proven by contradiction. Suppose not, then $\lambda_2 \geq \lambda_1 + 2$. Let $\lambda_3 = \lambda_1 + 1$. We must either have $2^{\lambda_3} \leq x$ or $x < 2^{\lambda_3}$. In the first case, this contradicts the claim that λ_1 is the maximal element of S_1. In the second case, this contradicts the claim that λ_2 is the minimal element of S_2.

Now, we axiomatise the rational numbers as an ordered field. We now refer to the set of rationals as $\mathbb{Q}$.

4. Prove that the floor relation is a well defined function for any $\frac{p}{q} \in \mathbb{Q}$. This can be thought of as the archimedean property for rationals.
Proof outline:
i. Prove that each rational number $\frac{p}{q}$ is bounded above and below by **integers**. For e.g. $\frac{|p|}{|q|} <\mid p \mid +1$
ii. Use well ordering principle as above, arrive at the desired conclusion.

5. How about the real numbers? With our axiomatic understanding that $\mathbb{Q}$ is an ordered field, we proceed to construct the real numbers R with Dedekind cuts. With this construction, we **prove** that R is an ordered field and obeys the axiomatic properties of an ordered field as well. Now, we refer to the sets of real numbers as $\mathbb{R}$.

6. Dedekind's construction of $\mathbb{R}$ also allows us to prove the lowest upper bound property of $\mathbb{R}$. With the lub property, we are now ready to prove the Archimedean property for $\mathbb{R}$. As a corollary of the archimedean property, we show that the floor function is well-defined on $\mathbb{R}$.

6 Number Theory

6.1 Main results

A list of the more useful lemmas and theorems.

6.1.1 Proposition 8.1.10

Let $d, n \in \mathbb{Z}$. If $d \mid n$ and $n \neq 0$, then $\mid d \mid \leq \mid n \mid$.

6.1.2 Lemma 8.1.14; Closure Lemma

Given integers a, b, m, n, d. If $d \mid m \wedge d \mid n$, then $d \mid (am + bn)$.

6.1.3 Proposition 8.1.12 (transitivity of divisibility)

6.1.4 Remark 8.2.2

1 is not prime. For $n \in \mathbb{Z}_{\geq 2}$, n is either prime or composite.

6.1.5 Lemma 8.2.4

An integer n is composite if and only if n has a divisor d such that $1 < d < n$.

6.1.6 Lemma 8.2.5 (Prime Divisor Lemma)

Let $n \in \mathbb{Z}_{\geq 2}$. Then n has a prime divisor.

6.1.7 Proposition 8.2.6

Let n be a composite positive integer. Then n has a prime divisor $p \leq \sqrt{n}$.

6.2 Other results

6.2.1 Tutorial 7 Q6

Let $a, b \in \mathbb{Z}$ with $a \neq 0, b \neq 0$. Then an integer n is a linear combination of a, b if and only if $\gcd(a, b) \mid n$.

This lemma can be used to prove the following result:
Consider the congruence equation $ax \equiv b \pmod{m}$. Then there exists solutions for x if and only if $\gcd(a, m) \mid b$.

Now suppose we have the congruence equation $ax \equiv b \pmod{m}$ and $\gcd(a, m) \mid b$ such that the equation is consistent. Then a general way to find solutions for x would be the following:

$$ax \equiv b \pmod{m} \iff \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

Since $\gcd(\frac{a}{d}, \frac{m}{d}) = 1$, we can use multiplicative inverses modulo $\frac{m}{d}$ to find values for x.

6.2.2 Multiplication related properties

Almost of the proofs for the following properties use Bezout's lemma.

- **Tutorial 7 Q2**
  Let $a, b \in \mathbb{Z}$. Suppose $a|c$ and $b|c$ and $\gcd(a, b) = 1$. Then $ab|c$.
- Suppose $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. Then $\gcd(a, bc) = 1$.
  This lemma is useful for proving the Chinese Remainder Theorem, showing that $\gcd(n_1, n_2n_3 \dots n_k) = 1$.

6.2.3 Chinese Remainder Theorem

See the article by Brilliant.

6.2.4 Number of trailing zeroes in factorial

First, let's solve the problem of finding the number of occurrences of a particular prime p in $n!$. Suppose the base p representation of n is $(c_kc_{k-1} \dots c_0)$. Then, number of occurrences =

$$\begin{aligned}
\sum_{k=1}^{\infty}\lfloor\frac{n}{p^k}\rfloor &= \sum_{1\leq j\leq k}\sum_{j\leq i\leq k} c_ip^{i-j} \\
&= \sum_{1\leq j\leq i\leq k} c_ip^{i-j} \\
&= \sum_{1\leq i\leq k}\sum_{1\leq j\leq i} c_ip^{i-j} \\
&= \sum_{1\leq i\leq k} c_ip^i \sum_{1\leq j\leq i}\frac{1}{p^i} \\
&= \frac{\sum_{1\leq i\leq k} c_i(p^i-1)}{p-1} \\
&= \frac{\sum_{1\leq i\leq k} c_ip^i - \sum_{1\leq i\leq k} c_i}{p-1} \\
&= \frac{\sum_{0\leq i\leq k} c_ip^i - \sum_{0\leq i\leq k} c_i}{p-1} \\
&= \frac{n - \text{(sum of digits in base-p representation of n)}}{p-1}
\end{aligned}$$

6.2.5 Manipulations involving modulo arithmetic

- Let $n = qd + r$. Then $n^k \equiv r^k(\mod d)$
- It is often useful to consider $(\mod 3)$. E.g. If a prime $p > 3$, then $p \equiv \pm1(\mod 3)$.
  We must also remind ourselves that in general, n can still be a prime even if $n \equiv 0(\mod p)$. This is when $n = p$. Hence the importance of the condition $n > p$.

7 Relations

7.1 Main results

7.1.1 Proposition 9.2.13

Let R be an equivalence relation on a set A. Then the following are equivalent $\forall x, y \in A$:

$$x\,R\,y$$
$$[x]_{\mathrm{R}} = [y]_{\mathrm{R}}$$
$$[x]_{\mathrm{R}} \cap [y]_{\mathrm{R}} \neq \emptyset$$

7.1.2 Definition 9.3.1

A partition P of a set A has 2 parts to its definition, namely existence and uniqueness.
For each element $x \in A$, there **exists** a **unique** element $S \in P$ such that $x \in S$.

7.1.3 Theorem 9.3.4

If R is an equivalence relation on a set A, then A/R is a partition of A.

7.1.4 Theorem 9.3.5

For a partition P of set A, there exists an equivalence relation R on A such that $A/R = P$

7.1.5 Characteristics

- Equivalence relations are reflexive, symmetric and transitive.
- Partial orders are reflexive, anti-symmetric and transitive.
- Total orders are partial orders and any 2 elements, not necessarily distinct, are comparable.

7.2 Converse relation

Usually called inverse relation in CS1231S.

- Given a relation $R : X \to Y$, and a predicate $P(x, y)$ such that $xRy \iff P(x, y)$.
  Then its inverse relation $R^{-1} : Y \to X$ is given by the following:

$$xR^{-1}y \iff yRx \iff P(y, x)$$

- Properties: (From Wikipedia)
  - If R is **reflexive, symmetric, antisymmetric, transitive, a partial order, total order, or an equivalence relation**, then R^{-1} is too.
  - A function is invertible if and only if its inverse relation is a function.

7.3 Complement relation

- Given a relation $R : X \to Y$, and a predicate $P(x, y)$ such that $xRy \iff P(x, y)$.
  Then its complement relation $R^c : X \to Y$ is given by the following:

$$xR^cy \iff x\not{R}y$$

7.4 Linearisation

Given a partial order $\preceq$ on set A, its linearisation is a total order $\preceq^*$ on A such that

$$\forall x, y \in A, (x \preceq y \implies x \preceq^* y)$$

For the positive integers, $\leq$ is a linearisation of $|$(divides), since $\forall x, y \in \mathbb{Z}^+, x|y \implies x \leq y$.
Note that if we consider the non-negative integers, this is not true. 0 is the largest element w.r.t $|$, but the smallest element w.r.t $\leq$.

7.5 Other tips

7.5.1 Check if relation is function

Given a relation

$$R : \mathbb{R} \to \mathbb{R}, \forall x, y \in \mathbb{R}, (xRy \iff x = \sin(y))$$

Is R or R^{-1} a function?

- We first look at R. Recall that when dealing with functions, we usually write them in the form $y = f(x)$, i.e. we bring y to the LHS for clarity, to show that y is the dependent variable. Hence, we write $\sin(y) = x$.
  Now it is clear that x ranges from -1 to 1, which is a strict subset of the domain $\mathbb{R}$. So R cannot be a function.
- For R^{-1}, we first write

  $$\forall x, y \in \mathbb{R}, xR^{-1}y \iff yRx \iff y = sin(x)$$

  Clearly, sin is a function, so R^{-1} is also a function.

7.5.2 Mistakes

- When writing out the ordered pairs comprising a partial order, don't forget the reflexivity. For e.g., on a Hasse diagram, there are no self loops, but we must remember that **partial orders are reflexive**, so for each element a on the diagram, $(a, a) \in \preceq$.
- When examining functions and relations, we must keep in mind the **domain** and **codomain**!

7.5.3 Coming up with examples

- Whenever we want to define a relation, we also need to define the relevant sets.
- Notice how the descriptors: reflexive, symmetric, antisymmetric, transitive etc. all use universal quantifiers. Hence, if we want a relation that is reflexive and symmetric and ... (i.e. meeting all the criteria), simply define $S = \emptyset$ and $R = \emptyset$ and let $R : S \to S$.
- Special cases:
  1. Empty set, empty relation. Then as previously mentioned, all universal descriptors are true.
  2. Non empty set, empty relation.
     - Not reflexive
     - Symmetric

  - Antisymmetric
  - Transitive

  Notice how all the universal conditional statements are vacuously true.

7.5.4 Set operations

- Union of reflexive relations is reflexive
- Union of symmetric relations is symmetric
- Union of transitive relations is **not** always transitive
- Union of antisymmetric relations is **not** always antisymmetric
- Intersection of reflexive, symmetric, transitive, antisymmetric relations are always reflexive, symmetric, transitive, antisymmetric respectively.

8 Permutations and combinations

8.1 Proving equality of counting methods

We will use an example to demonstrate this.

8.1.1 Tutorial 9 Qn 7a

In how many ways can 8 boys and 4 girls sit around a circular table, so that no two girls sit together?

First we conjecture the following method of counting by viewing this as a 2-step process:
Step 1: Seat the 8 boys in a circular permutation.
Step 2: Insert the 4 girls in between the 8 boys.

$$\begin{aligned} n_1 &= (8-1)! \\ n_2 &= P(8,4) \\ \text{By Product Rule, } n_1 n_2 &= \frac{7!8!}{4!} \end{aligned}$$

Why is this 2-step process the correct way of arranging 8 boys and 4 girls together such that no girls are adjacent? To prove this, we can follow the following steps:
1. Prove that our conjectured method of counting has no double-counting, i.e. it forms a set without repetition. Consider 2 outputs O1, O2 that are produced by the 2-step process.
Case 1: Suppose O1, O2 were the same after Step 1.
Then, O1, O2 must differ in the Step 2, such that the seating of the girls is different. Then, clearly O1 and O2 are distinct ways of arranging seats.
Case 2: Suppose O1, O2 differ in their Step 1 of construction.
Then regardless of how the girls are removed, the boys are ordered differently. Hence O1≠O2.
Now, we have proven that no double counting takes place. We now prove that this set S_1 of arrangements produced is precisely the set S_2 of all valid arrangements.
$(S_1 \subseteq S_2)$: Suppose $x \in S_1$. Then obviously, x is a valid arrangement. Hence, $x \in S_2$.

$(S_2 \subseteq S_1)$: Suppose $x \in S_2$. Then, if we temporarily remove the girls, we get a circular permutation of the 8 boys. This can be produced by Step 1 of our counting method. Now, we consider the girls. The 4 girls are inserted between the 8 boys, so this can also be produced by Step 2 of our counting method. Hence, $x \in S_1$.

8.1.2 In Summary

The method described above can be clearly stated (and generalised slightly) as follows:

Double counting Suppose we have 1 way of counting that forms a set A, and we want to show that the 2nd way of counting is counting the same quantity,

1. Show that the 2nd way of counting does not over-count, i.e. the 2nd way of counting produces a set B. Now we want to show either A has a 1-1 correspondence to B or $A = B$.
2. Method 1: Establish a bijection between A and B
   (a) Show that each element in A corresponding to an element in B (i.e. define a mapping from $A \to B$.
   (b) Show that this mapping is injective and surjective.
3. Method 2: Show set equality directly (Note that this is a special case of method 1. Here, the mapping is the identity map.)
   (a) Show $x \in A \implies x \in B$ and $x \in B \implies x \in A$

8.2 Random variables

From math.stackexchange
Given a universal sample space $\Omega = \{\omega_i, 1 \leq i \leq n\}$, where ω_i are the events.
Define a function

$$\begin{aligned} X :& \Omega \to \mathbb{R} \\ & \omega_i \mapsto X(\omega_i) \end{aligned}$$

$X(\omega_i)$ is value of the random variable X at the event $\omega_i \in \Omega$.

8.3 Linearity of expectation

Given random variables X, Y which may be dependent, $E(X+Y) = E(X) + E(Y)$

8.4 Law of Total/Iterated Expectation

From Wikipedia
If X is a random variable whose expected value $E(X)$ is defined, and Y is any random variable on the same probability space, then

$$E(X) = E(E(X|Y))$$

In one special case, if $\{A_i\}$ is a finite or countable partition of the sample space, then

$$E(X) = \sum_i E(X|A_i)P(A_i)$$

8.5 Other problems

8.5.1

Given n_1 distinct items of type 1, n_2 distinct items of type 2, ..., n_j distinct items of type j.

1. How many ways are there to select k_1 items of type 1, ..., k_j items of type j to form an unordered set? Note that order of choice does not matter.

- $$C(n_1,k_1)C(n_2,k_2)\dots C(n_j,k_j)$$

2. How many ways are there to select k_1 items of type 1, ..., k_j items of type j to form an ordered tuple?
   - Think of this as a 2 step process:
   - First, we find the number of unordered sets we can make (i.e. using the counting method in (1). Note that since each of these unordered sets are different, any two ordered tuples/arrangements each originating from a different set must also be different. This says that unordered sets are "disjoint" when we permute them subsequently in the next step.
   - Now, each set has $K = \sum_{i=1}^{j} k_i$ distinct elements. Hence, there are $K!$ permutations of each.
   - Hence, number of ways $= C(n_1,k_1)C(n_2,k_2)\dots C(n_j,k_j)K!$

3. What is the probability of a choice (unordered) of items from all $N = \sum_{i=1}^{j} n_i$ items having k_1 items of type 1, ..., k_j items of type j?
   - $$\frac{C(n_1,k_1)C(n_2,k_2)\dots C(n_j,k_j)}{C(N,K)}$$
   - Alternatively, we can consider this:
   - The probability that the first k_1 selections are of type 1, the next k_2 selections are of type 2, ... , last k_j selections are of type j is $\frac{P(n_1,k_1)P(n_2,k_2)\dots P(n_j,k_j)}{P(N,K)}$
   - In fact, we can define

     $$E_{i_1,i_2,\dots,i_K},\ 1 \le i_1, i_2, \dots, i_K \le j$$

     as the event where when choosing K items, the first item is of type i_1, second item is of type i_2, and so on. Then by writing out the fractions, and compressing the numerator and denominator, we have $P(E_{i_1,i_2,\dots,i_K}) = \frac{P(n_1,k_1)P(n_2,k_2)\dots P(n_j,k_j)}{P(N,K)}$ for all choices of $i_1, i_2, \dots, i_K$
   - We now need to find all possible permutations of $1 \le i_1, i_2, \dots, i_K \le j$, where there are k_1 1's, k_2 2's, and so on. Here, we need to view objects of the same type as indistinguishable. There are $\frac{K!}{k_1!k_2!\dots k_j!}$ ways.
   - Multiplying, we get

     $$\frac{P(n_1,k_1)P(n_2,k_2)\dots P(n_j,k_j)}{P(N,K)} \cdot \frac{K!}{k_1!k_2!\dots k_j!} = \frac{C(n_1,k_1)C(n_2,k_2)\dots C(n_j,k_j)}{C(N,K)}$$

8.5.2 Handshake Theorem

Let $G(V,E)$ be a graph. The sum of degrees of all vertices of G equals twice the number of edges in G. Specifically, if the vertices of G are $v_1, v_2, \dots, v_n$, where $n \ge 0$, then

$$\text{Total degree of } G = 2 * |E|$$

Proof by double counting

1. Consider the set S of tuples (v_i, e_j), which lists out every pair of vertex v and edge e in the graph that is connected.
2. Consider the LHS, to get the total degree of G, we sum deg(v_1)+...+deg$(v_{|V|})$. By doing this, we are partitioning the set S described in step 1 into $|V|$ subsets (note that some of these can be empty) and applying the addition principle.
3. Consider the RHS, here we partition S into $|E|$ non-empty sets. Each set must contain precisely 2 elements, $(v_{i1}, e_j), (v_{i2}, e_j)$ since an edge connects precisely 2 vertices. Hence, applying addition principle again, $|S| = \sum_{1\leq i\leq |E|} 2 = 2 * |E|$.
4. By the double counting argument, we have total degree of $G = 2 * |E|$.

8.5.3 Functions

Consider 2 sets X and Y, where $|X| = m$, $|Y| = n$.

- Number of function $f : X \to Y$
  - n^m
- Number of injective functions $f : X \to Y$
  - Consider the following method of counting:
  - List out the elements in domain X as $x_1, x_2, \ldots, x_m$
  - There are n choices of image for x_1, $n-1$ choices for x_2, ...
  - Hence, by product rule, there are $n(n-1)\ldots(n-m+1) = nPm$ such functions if $m \leq n$.
  - Note that if $m > n$, there are 0 injective functions by pigeonhole principle.
- Number of surjective functions $f : X \to Y$
  - List out the elements in domain X as $x_1, x_2, \ldots, x_m$
  - Define X_i as the set of functions from $X \to Y$ that have x_i in their image
  - We want to find

    $$|\cap_{1\leq i\leq n} X_i|$$

  - By addition principle,

    $$|\cap_{1\leq i\leq n} X_i| = |S| - |\cup_{1\leq i\leq n} \overline{X_i}|$$

    where $|S| = n^m$
  - Using PIE:

    $$\begin{aligned} |\cup_{1\leq i\leq n} \overline{X_i}| &= \sum_{1\leq i\leq n} |\overline{X_i}| - \sum_{1\leq i<j\leq n} |\overline{X_i \cap X_j}| + \ldots \\ &= \sum_{1\leq i\leq n} (n-1)^m - \sum_{1\leq i<j\leq n} (n-2)^m + \ldots \\ &= \binom{n}{1}(n-1)^m - \binom{n}{2}(n-2)^m + \binom{n}{3}(n-3)^m - \ldots \\ &= \sum_{i=1}^{n} (-1)^{i-1}\binom{n}{i}(n-i)^m \end{aligned}$$

- Hence,

$$\begin{aligned}
|\cap_{1\leq i\leq n} X_i| &= n^m - \sum_{i=1}^{n}(-1)^{i-1}\binom{n}{i}(n-i)^m \\
&= n^m + \sum_{i=1}^{n}(-1)^{i}\binom{n}{i}(n-i)^m \\
&= \sum_{i=0}^{n}(-1)^{i}\binom{n}{i}(n-i)^m \\
&= m!S(n,m)
\end{aligned}$$

- Number of bijective functions:
  - We can prove by pigeonhole principle that there exists bijection between X and Y if and only if $m = n$.
  - If $m = n$, then any mapping $f : X \to Y$ is injective $\iff$ f is bijective.
  - Hence, it suffices to count the number of injective functions, which is $nPn = n!$

8.5.4 Special numbers

1. Binomial coefficients
   - Pascal's identity:

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

   - Combinatorial proof: Let S be the set of all k-combinations (i.e. subsets of size k) from a pool of n distinct elements. Partition S into 2 components, A and B, where the k-combinations in A have a particular element x_0 and the k-combinations in B do not. By addition principle, $|S| = |A| + |B|$.
2. Stirling numbers of the first kind
3. Stirling numbers of the second kind
   - $S(n,k)$ is the number of ways of putting n labelled items into k unlabelled boxes.
   - Note that $k!S(n,k)$ is the number of surjective functions from n elements in the domain to k elements in the codomain. This is as if we are labelling the boxes and permuting the labels.
   - Recurrence relation:

$$S(n,k) = kS(n-1,k) + S(n-1,k-1)$$

   - Other identities:

$$S(n,n-1) = \binom{n}{2}$$

$$S(n,2) = \frac{1}{2}(2^n - 2) = 2^{n-1} - 1$$

8.5.5 Circular permutations

Seating around an **unnumbered** round table.
In general, this is not an easy problem.
In general, if we have m object of k types, r_i items of the i-th type for $1 \leq i \leq k$, we cannot use the linear permutation formula to say that there are $\frac{(m-1)!}{r_1!r_2!\ldots r_k!}$ permutations.
One reason for this: When we consider objects of the same type to be distinct (temporarily, i.e. we divide later one), permuting the object of 1 type can change the relative positioning with respect to objects of other types.

An example of a difficult problem: Bracelet with n white balls and m black balls
Even with just 2 types of indistinguishable objects, this problem is already far beyond our abilities(at this point).

However, there are certain simple cases in which we can use the product rule (in a relatively simple manner). Consider the following examples:

- Seating k people around a table with n seats. Here, the people are clearly all distinct. There is only 1 type of indistinguishable object: the $n - k$ empty chairs.
  - Edge case: If $k = 0$, there is only 1 way.
  - If $1 \leq k \leq n$, then there are $\frac{(n-1)!}{(n-k)!}$ ways. Notice that $(n - k)$ is the number of empty seats.

8.5.6 Order of choice

CS1231S Quiz How many (3) - digits even integer can you create if the digits are picked from (0,2,4,5,7,8) and no repetitions are allowed?
Strategy:

1. Split into 2 cases:
2. Case 1: With 0 in 1's place.
   There are then 4P2 choices for the other 2 digits.
3. Case 2: With no 0 in 1's place.
   There are 3 choices(2,4,8) for the even digit in the 1's place.
   Then, we choose the digit in the hundredth place. This cannot be 0, so there are 4 choices.
   Finally, choose the digit in the tenth place. There are 4 choices, since 0 can be in the tenth place.

This can easily be generalised to more digits.

8.5.7 Counting divisors

Given two integers a and b, where $a \leq b$, how many divisors of k are there in $[a, b]$?

$$\lceil \frac{a}{k} \rceil \ldots \lfloor \frac{b}{k} \rfloor$$

Hence, $max(0, \lfloor \frac{b}{k} \rfloor - \lceil \frac{a}{k} \rceil + 1)$ divisors

8.6 Pigeonhole Principle

8.6.1 Links to explore

- Cut the Knot
- CS Cornell CS280 PP problems

8.6.2 Covering problem

Given a road of length l, and that each router has a maximum network radius of d, what is the minimum number of routers needed to cover the whole road? (Think of this as forming the smallest possible surjection from the set of routers to the set of road segments)

1. Divide the road into $\lfloor \frac{l}{2d} \rfloor$ segments of size $2d$, with $\lceil \frac{l}{2d} \rceil - \lfloor \frac{l}{2d} \rfloor$ leftover segments. Altogether, there are $\lceil \frac{l}{2d} \rceil$ segments of maximum length $2d$.
2. We claim that the minimum number of routers is $\lceil \frac{l}{2d} \rceil$.
3. To show that this number of routers leads to a viable covering, we simply place one router in the center of each segment.
4. Now, suppose that we have fewer routers than $\lceil \frac{l}{2d} \rceil$. Then there must be a segment without a router.
5. (Justification by PP) Let the pigeons be the segments, routers be the pigeonholes, then as number of pigeons exceed number of pigeonhole, there exist some pigeonholes with >= 2 pigeons, i.e. some router has at least 2 segments mapped to it. Then one of these segments does not have a router. In other words, it is not possible to form a surjection from the router to the segments.
6. Alternatively, use the contrapositive of PP. For there to be a surjection from the router to the segments, each segment must have at least 1 router that maps to it. By the contrapositive of PP, the number of routers must be greater or equal to the number of routers.
7. Stand in the center of that segment without a router. Then there will be no connection there and hence this is an invalid placing of routers.

8.6.3 Packing problem

Given n chairs in a row and that 2 people must sit minimally k distance apart, what is the maximum number of people that can sit down? (Think of this as forming the largest possible injection from the set of people to the set of chairs)

1. Divide the n chairs into $\lfloor \frac{n}{k+1} \rfloor$ segments of size $k+1$, with $\lceil \frac{n}{k+1} \rceil - \lfloor \frac{n}{k+1} \rfloor$ leftover segments. Altogether, there are $\lceil \frac{n}{k+1} \rceil$ segments of maximum size $k+1$.

8.6.4 Set duplication

9 Graphs

9.1 Definitions

A few things to note:

1. - The existence of a walk from vertex u to vertex v implies the existence of a trail and a path from u to v.
   - However, the existence of a closed walk starting and ending at vertex v does not necessarily imply a closed circuit starting and ending at vertex v. Because for e.g. $v_1 \to v_2 \to v_1$ using the same edge is a closed walk, but not a circuit.
   - However, note that a closed walk of **odd** length will contain a circuit. Since we obviously can't have the trivial case $v_1 \to v_2 \to v_1$ as shown above.

9.2 Theorems

1. Euler's formula for connected planar simple graphs

$$f = e - v + 2$$

   - A particular case of this is trees, where $e = v - 1$ and $f = 1$
   - We know trees are connected and simple graphs. To prove that they are planar, we use induction:
   -

2. Number of spanning trees in a complete graph $K_n = n^{n-2}$

9.3 Hamiltonian graphs

A relatively easy way to check for non-existence of a Hamiltonian cycle, Consider the graph B in page 49 of the lecture slides.

- We first suppose graph B has a Hamiltonian cycle (to obtain a contradiction).
- Then since it is a cycle, it doesn't matter where we start. We should be able to obtain the same Hamiltonian cycle starting from any point in the graph.
- Consider the bottom vertex of degree 2. Since we must enter and exit this vertex, any Hamiltonian cycle must include both edges connected to this vertex.
- Then consider the vertex right above the bottom vertex. This vertex also is of degree 2. Hence, both edges connected to it must be included in the Hamiltonian cycle.
- The trick: Notice that the 4 edges we have included in the Hamiltonian cycle form a cycle amongst themselves. This is not possible since a Hamiltonian cycle is a simple cycle (with no vertex repetition), such that any proper subset of the Hamiltonian cycle cannot be a cycle.

9.4 Binary Tree Construction

9.4.1 From preorder and inorder

- Let T be a binary tree. Suppose we are given a preorder traversal sequence A and an inorder traversal sequence B.
- We can always construct T by starting from the start of sequence A.
- Why? The first element of A must be the root, since the root is where we start our preorder traversal, so there is no ambiguity in its location.
  Due to the nature of preorder traversal, parent vertices are always reached and recorded before child vertices, hence at any point in the construction, the current element e in sequence A must be adjacent to one of the vertices in the partially constructed tree because e's parent must have been reached and included in the partial tree already.

9.4.2 From postorder and inorder

- Let T be a binary tree. Suppose we are given a postorder traversal sequence A and an inorder traversal sequence B.
- We can always construct T by starting from the end of sequence A and going backwards.

- Why does this work? Consider postorder traversal. The last element of A must be the root, so there is no ambiguity in its location. Any other element of A is not the root, and hence must have a parent.
  The nature of postorder traversal is that parent vertices are always recorded after child vertices, hence when the current element e of A is reached, (as we started from the back of A) the parent of e must be included in the partial tree already.

In both cases (9.4.1 and 9.4.2), at each stage of the construction, the partial tree partitions the space into disjoint intervals. The presence of the inorder traversal means that there is no ambiguity as to where to place the next element e.