CS 70

Discrete Mathematics and Probability Theory

Lecture Notes

Textbook: Lehman's *Mathematics for Computer Science*

DRUV PAI
druvpai@berkeley.edu
ID: SID: 3033848822

PROFESSOR: TBD
GSI: TBD

Contents

1 Lecture 1

Some logistics are on the course website.

Propositions and First Order Logic

Assume a set of cards C, where each card contains a name N, destination D, and mode of travel T. Consider the assertion "fix a d in D and t in T, and for each n in N if the corresponding destination is d then the mode of travel is t". This is a proposition.

Definition 1
A **proposition** is a statement that can be assigned an objective truth value (true or false).

We can put propositions together to make another.

- **conjunction** ("and"): $P \land Q$, true when both P and Q are true, or else false.
- **disjunction** ("or"): $P \lor Q$, true when at least one of P or Q is true, or else false.
- **negation** ("not"): $\neg P$, true when P is false and false otherwise.

Note that conjunction and disjunction are commutative. Using conjunctions we can get ridiculously long statements.

Here are the truth tables for the previous operations.

P	Q	$P \land Q$
True	True	True
True	False	False
False	True	False
False	False	False

P	Q	$P \lor Q$
True	True	True
True	False	True
False	True	True
False	False	False

P	$\neg P$
True	False
False	True

One use for truth tables is to determine the logical equivalence of propositional forms. For example, $\neg(P \land Q)$ is logically equivalent to $\neg P \lor \neg Q$ because they have the same truth table.

Theorem 2 (DeMorgan's Law)
For a given logical expression, we can "distribute" not-forms by interchanging "and" with "or" and pre-pending "not" to every term.

Another consequence is that True $\land Q \equiv Q$ and that False $\lor Q \equiv Q$. On the other hand, False $\land Q \equiv$ False and True $\lor Q \equiv$ True.

Example 3
Verify the logical equivalence

$$P \land (Q \lor R) \equiv (P \lor Q) \land (P \lor R)$$

which acts as a distributive property.

Solution. We use casework. If P is true, then the left hand side becomes $Q \lor R$ and the right hand side becomes (True $\land Q$) $\lor$ (True $\land R$) $\equiv Q \lor R$. If P is false then the left hand side is False and the right hand side is (False $\land Q$) $\lor$ (False $\land R$) $\equiv$ False. □

We can use this property to simplify many other logical equivalences.

Another important logical operation is implication ("if-then"). That is, $P \implies Q$ is "if P then Q". If P is true, and $P \implies Q$, then Q is true.

The statement $P \implies Q$ is only false if P is true and Q is false. If P is false, Q can be true or false. When Q is true, P can be true or false.

Some alternative verbiage for implication is

- "if P then Q"
- Q if P
- P only if Q
- P is sufficient for Q
- Q is necessary for P

Interestingly, $P \implies Q$ is the same as $\neg P \vee Q$.

The **contrapositive** of $P \implies Q$ is $\neg Q \implies \neg P$.

Example 4

A proposition and its contrapositive are logically equivalent.

Proof. In one line:

$$P \implies Q \equiv \neg P \vee Q \equiv \neg(\neg Q) \vee \neg P \equiv \neg Q \implies \neg P$$

as claimed. ■

The **converse** of $Q \implies Q$ is $Q \implies P$. A proposition and its converse are not logically equivalent.

If $P \implies Q$ and $Q \implies P$ then $P \iff Q$ ("**if-and-only-if**"). In other words, P if and only if Q means that P is true if and only if Q is true, or else it is false.

A proposition that depends on one or more variable is a **predicate**. The notation is $P(x)$. An example is $P(n) \overset{\text{def}}{=} \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, but note that the predicate does not necessarily need to be true.

The **there exists** quantifier means that there is at least one value of a variable such that the predicate is satisfied. The notation is $(\exists x \in S)(P(x))$. An example is $(\exists x \in \mathbb{N})(x = x^2)$.

The **for all** quantifier means that all values of a variable satisfy the predicate. The notation is is $(\forall x \in S)$. An example is $(\forall x \in \mathbb{R})(x < x+1)$.

The **universe** of an assertion containing one or more variables is the domain or domains of the variables involved in the predicate.

We'll now cover some more examples of "for-all" quantifiers, and their negations.

- $(\forall x \in \mathbb{N})(2x > x)$ is false, consider $x = 0$. The true claim is $(\forall x \in naturals)(2x \geq x)$.
- $(\forall x \in \mathbb{N})(x > 5 \to x^2 > 25)$ is true.
- $(\exists y \in \mathbb{N})(\forall x \in \mathbb{N})(y = x^2)$ is false. This means "there is a natural number that is the square of every natural number". Switching the order of quantifiers yields $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(y = x^2)$ which asserts that the square of a natural number is a national number, which is true.

This leads to the following example:

Example 5

Switching the order of quantifiers can affect the truth value of the statement; quantifiers are not commutative.

Now we deal with assertion. Consider the claim

$$\neg(\forall x \in S)(P(x))$$

which is true when there's at least one counterexample. Therefore,

$$\neg(\forall x \in S)(P(x)) \iff \exists(x \in S)(\neg P(x))$$

Corollary 6 (DeMorgan's Law)
Negation of a quantifier switches it to the other quantifier. That is,

$$\neg(\forall x) \equiv \exists x \quad \text{and} \quad \neg(\exists x) \equiv \forall x$$

and

$$\neg((\forall x)(P(x))) \equiv (\exists x)(\neg P(x)) \quad \text{and} \quad \neg((\exists x)(P(x))) \equiv (\forall x)(\neg P(x))$$

2 Lecture 2

Today, we cover proofs. There are some methods:

- By example.
- Direct. (Prove $P \implies Q$).
- By contraposition (Prove $\neg Q \implies \neg P$).
- By contradiction. Prove $\neg P$ given a consequence of Q.
- Induction.

We work mostly with the integers, and we will cover some properties and notation.

- The integers are closed under addition. That is, $a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z}$
- When a divides b, or b is **divisible** by a, we have that $\exists q \in \mathbb{Z}$ such that $b = aq$.
- A natural number $p > 1$ is **prime** if it is divisible only by 1 and itself.

Direct Proofs

We start with some examples.

Example 7
For any $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$ then $a \mid (b - c)$.

Proof. Assume $a \mid b$ and $a \mid c$. Then $b = aq$ and $c = aq\prime$ where $q, q\prime \in \mathbb{Z}$. Then

$$b - c = a(q - q\prime) \quad \text{and} \quad q - q\prime \in \mathbb{Z} \implies a \mid (b - c)$$

This argument applies for every $a, b, c \in \mathbb{Z}$. ■

What we did was a direct proof. Our goal was to show that $P \implies Q$, so we assume P and show that the consequences of P include Q.

Example 8
Let D_3 be the set of three-digit natural numbers. For $n \in D_3$, if the alternating sum of digits of n is

divisible by 11, then $11 \mid n$. In other words,

$$(\forall n \in D_3)(11 \mid \text{alternating sum of digits of } n \implies 11 \mid n)$$

Proof. By a base expansion, there exist $a, b, c \in \mathbb{N}$ such that

$$n = 100a + 10b + c$$

By the example statement, there exists $k \in \mathbb{Z}$ such that

$$a - b + c = 11k$$

Adding $99a + 11b$ to both sides, we have

$$100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b)$$

Since the integers are closed under addition, $k + 9a + b \in \mathbb{Z}$ so $11 \mid n$. ■

This is another direct proof. We'll now try the converse.

Example 9

Let D_3 be the set of three-digit natural numbers. For $n \in D_3$, if $11 \mid n$, then the alternating sum of digits of n is divisible by 11. In other words,

$$(\forall n \in D_3)(11 \mid n \implies 11 \mid \text{alternating sum of digits of } n)$$

Proof. Assume $11 \mid n$. Then

$$n = 100a + 10b + c = 11k \implies a - b + c = 11k - 99a - 11b = 11(k - 9a - b)$$

Since the integers are closed by induction, $k - 9a - b$ is an integer, so $11 \mid (a - b + c)$, completing the proof. ■

This is a similar proof to the first proof. In this case, every implication is a two-way implication. This is often the case with arithmetic properties, not by multiplying by zero.

Thus, we have the example

Example 10

Let D_3 be the set of three-digit natural numbers. For $n \in D_3$, the alternating sum of digits of n is divisible by 11 if and only if $11 \mid n$. In other words,

$$(\forall n \in D_3)(11 \mid \text{alternating sum of digits of } n \iff 11 \mid n)$$

Proof by Contraposition

Again, we begin with some examples.

Example 11

For $n \in \mathbb{N}^+$ and $d \mid n$, if n is odd, then d is odd.

Proof. We use the method of contraposition. Assume that d is even, so $d = 2k$. Then

$$n = qd = 2qd$$

so n is even. Thus the contrapositive, and the statement itself, are both true. ■

Example 12
For every $n \in \mathbb{N}$, n^2 being even implies n is even.

Proof. We use proof by contraposition. Assume that n is odd, so $n = 2k+1$ for some integer k. Then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$$

which is an odd number (since the first two terms are both divisible by 4 and thus 2). Thus the contrapositive and the statement itself are both true. ■

Proof by Contradiction

Example 13
The number $\sqrt{2}$ is irrational. In other words, for all $a, b \in \mathbb{N}$, we have $(a+b)^2 \neq 2$.

Proof. We use contradiction. Assume $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$. Further assume without loss of generality that a, b have no common factors. Then

$$\sqrt{2}b = a \to 2b^2 = a^2$$

By Example 2.6, a^2 is even implies a is even. So write $a = 2k$ for some integer k. Then

$$2b^2 = a^2 = (2k)^2 = 4k^2 \to b^2 = 2k^2$$

Since b^2 is even, b is even. Since a and b are both even, they share a common factor. This is a contradiction, so $\sqrt{2}$ is irrational. ■

The key behind proof by contradiction is to prove from the opposite of the proposition $\neg P$ the assertions Q and $\neg Q$. Since $P \implies Q \wedge \neg Q \equiv$ False, the contrapositive implies True $\implies P$.

Example 14
There are infinitely many prime numbers.

Proof. We use contradiction. Assume that there exist only n primes $p_1, \ldots, p_n$. Then consider

$$q = 1 + \prod_{k=1}^{n} p_k = 1 + x$$

Since it's larger than any prime number, q is not prime. So q has at least one (without loss of generality, assume one) prime divisor p. Then p divides both x and q. By Example 2.1, p divides $x - q$, which by definition is 1. But for p to divide 1, it must be 1, which is a contradiction to p being a prime. ■

Proof by Cases

Example 15
The equation $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof. First, a lemma:

Lemma. If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in \mathbb{Z}$, then both a and b are even.

Proof. Assume a solution of the form a/b in lowest terms, and get:

$$\left(\frac{a}{b}\right)^5 - \frac{a}{b} + 1 = 0$$

Multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

We use casework:

- Case 1: a, b odd, odd - odd + odd = even, impossible.
- Case 2: a even, b odd: even - even + odd = even, impossible.
- Case 3: a odd, b even: odd - odd + even = odd, impossible.
- Case 4: a, b even: even - even + even = even, possible.

■

Since a, b are not in lowest form, there's a contradiction. ■

Example 16
There exist irrational x and y such that x^y is rational.

Proof. Let $x = y = \sqrt{2}$. We have two cases:

- Case 1: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational.
- Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Then we try $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$. Then

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$$

Thus, we have irrational x and y with rational x^y. ■

Induction

We can use induction on statements about all natural numbers:

$$(\forall n \in \mathbb{N})(P(n))$$

The **Principle of (Weak) Induction** means that $P(0)$ and $P(k) \implies P(k+1)$ implies $P(k)$ for all integers k. The method of induction is to

1. Prove $P(0)$ (base case).
2. Assume $P(k)$ (induction hypothesis).
3. Prove $P(k+1)$ (induction step).

Example 17 (Gauss)
For all natural numbers n, $\sum_{k=0}^{n} k = n(n+1)/2$.

Proof. We use induction. Our base case is $n = 0$, where $0 = 0(0+1)/2$. Our induction step is to show that for all $k \geq 0$, $P(k) \implies P(k+1)$. The induction hypothesis is

$$P(k) \overset{\text{def}}{\equiv} \sum_{j=1}^{k} j = \frac{k(k+1)}{2}$$

The induction step is

$$P(k+1) \equiv \sum_{j=0}^{k+1} j = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)+2k+2}{2} = \frac{(k+1)(k+2)}{2}$$

Hence, the induction hypothesis is satisfied for $k+1$, so $P(k)$ implies $P(k+1)$, and so we are done. ■

3 Lecture 3

Today, we continue with the principle of induction.

Weak Induction

In the coarsest view, the principle of induction can be written as

$$(P(0)) \wedge ((\forall n \in \mathbb{N})(P(n) \implies P(n+1))) \implies (\forall n \in \mathbb{N})(P(n))$$

In general, $P(n) \neq P(n+1)$, so there's no circular logic here. We plug in a base case to $P(0)$, prove that it holds, then fix an n and prove $P(n) \implies P(n+1)$.

Example 18
For every $n \in \mathbb{N}$, $n^3 - n$ is divisible by 3. ($3 \mid (n^3 - n)$).

Proof. We use induction. The base case is $n = 0$, and $3 \mid 0$. Now assume that it's true for $n = k$; in particular, write $k^3 - k = 3q$, and we attempt to prove that it holds for $k+1$. We have

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 2k = (k^3 - k) + 3k^2 + 3k = 3q + 3k^2 + 3k = 3(q + k^2 + k)$$

Since the integers are closed under addition, $q + k^2 + k$ is an integer, so $(k+1)^2 - (k+1)$ is divisible by 3. Since $P(k)$ implies $P(k+1)$, we are done. ■

Theorem 19 (Four Color Theorem)
Any map can be colored so that those regions that share an edge have different colors, and we need to use at most four colors assuming that one region is not completely contained in another.

Example 20
Define a proper coloring of a map as an assignment of colors to contiguous regions in which no two regions that share an edge have the same color.

Any map formed by dividing the plane into regions by drawing straight lines can be properly colored with two colors.

Proof. We prove this using induction. First of all, dividing the plane into two regions is trivially able to be properly colored; assign different colors to the two regions.

Now onto the inductive step. Add a line in the plane, and the new regions inherit their old colors that they had without the new line. Then swap the colors of all regions on one side of the new line, which fixes conflicts along the line, and makes no new conflicts. ■

Example 21
The sum of the first n odd numbers is n^2.

Proof. We use induction. Define the kth odd number as $2(k-1)+1$.

The base case is that $1 = 1^2$, which is obviously true.

Now assume that the sum of the first k odds is the perfect square k^2. Then we add $2((k+1)-1)+1 = 2k+1$ to k^2, and get

$$k^2 + 2k + 1 = (k+1)^2$$

This implies that the sum of the first $k+1$ odd numbers is $(k+1)^2$. By induction, we are done. ■

Example 22
Show that we can tile a $2^n \times 2^n$ grid with L-shaped width-1 pieces, with exactly one 1×1 hole.

Proof. The statement is proved due to the fact that the remainder of $2^n \times 2^n = 2^{2n}$ divided by 3 is 1. We use induction for this.

Our base case is that $n = 0$, so $2^{2(0)} = 1$ which has remainder 1 when divided by 3. Now assume it's true for $n = k$, then we have

$$2^{2k} = 3m + 1$$

and so

$$2^{2(k+1)} = 4(2^{2k}) = 4(3m+1) = 12m + 4 = 3(4m+1) + 1$$

which has a remainder of 1 when divided by 3, as claimed. By induction, we are done. ■

We prove a stronger version here.

Example 23
We can tile the $2^n \times 2^n$ square with a singular hole, leaving the hole at any point in the grid.

Proof. We use induction.

The base case is that a single tile works fine. The induction hypothesis is that a $2^n \times 2^n$ square can be tiled with a hole anywhere. Now, consider a $2^{n+1} \times 2^{n+1}$ square. Cut the courtyard in four pieces, and use the induction hypothesis in each, placing the holes in the corners near the center for all sections not containing the hole. Then use an L tile to cover the L shape formed by the holes in the middle.

This algorithm provides a way to tile the $2^n \times 2^n$ square with an arbitrary hole, for any n. ■

Strong Induction

We begin with a motivated example.

Example 24 (Fundamental Theorem of Arithmetic)
Every natural number $n > 1$ can be written as a (possibly trivial) product of primes.

Proof. We use strong induction. Let $P(n)$ be the statement that n can be written as a product of primes.

The base case is $n = 2$, which is trivially prime.

Now we use the induction step. Assume n can be written as a product of primes. Either $n+1$ is a prime or $n+1 = ab$ where $1 < a, b < n+1$. If $n+1$ is prime, we're done, so say $n+1 = ab$. Then $P(a)$ and $P(b)$ are true by strong induction, so multiplying together their prime factors yields that n can be written by a product of primes. ■

This shows the **Principle of Strong Induction**, which means that $P(0)$ and $\bigwedge_{i=0}^{k} P(i) \implies P(k+1)$ implies $P(n)$ is true for all natural numbers n.

If $(\forall n)(P(n))$ is not true, then there exists n such that $\neg P(n)$. Then there must be a smalest m with $\neg P(m)$, so $P(m-1) \not\Longrightarrow P(m)$. This is just the contrapositive of the induction principle.

Theorem 25 (Well Ordering Principle)
For any subset of the natural numbers there exists a smallest element.

Example 26
We define a round robin tournament on n players as a set of games in which every player plays every other player and each game has a winner.

We define a cycle as a sequence of $p_i, \ldots, p_j$ where each player beats the player to their right.

Every tournament that has a cycle has a cycle of length 3.

Proof. Assume that the smallest cycle is of length k. We use cases.

The state $k = 0$ means we're done, while $k = 1$ is meaningless.

The state $k = 2$ is impossible since each player plays every other once, so there's no back-and-forth.

If $k = 3$, we're done.

If $k > 3$, then we can either:

- always draw a cycle between the initial, second, and last elements, so we can find a cycle of length 3, a contradiction.
- draw a cycle of length $k - 1$ which avoids the initial element, which is a contradiction.

Hence, the statement is proved.

■

Example 27
Use the same definition as above. Define a Hamiltonian path as a sequence $p_1, \ldots, p_n$, where for all i such that $0 \leq i \leq n$, p_i beats p_{i+1}.

Every tournament has a Hamiltonian path.

Proof. We use induction. The base case is $n = 2$, which is true. Now assume $n = k$ is true, and attempt to prove it for $k+1$. Removing a player p from the tournament on $k+1$ people yields a tournament on k people. By the induction hypothesis there's a Hamiltonian path on $p_1, \ldots, p_n$.

If p beats everyone, put p at the beginning; if p loses to everyone, put p at the end. Else, put p at the first place i where p beats p_i. Then $p_1, \ldots, p_{i-1}, p, p_{i+1}, \ldots, p_n$ is a Hamiltonian path. ■

4 Lecture 4

Strong Induction and Recursion

We begin with an example.

Example 28
For every natural number $n \geq 12$, there exist natural x and y such that $n = 4x + 5y$.

Proof. Here's some code:

```
def find-x-y(n):
    if (n==12) return (3, 0)
    elif (n==13): return (2,1)
    elif (n==14): return (1,2)
    elif (n==15): return (0,3)
    else:
        (x', y') = find-x-y(n-4)
        return (x'+1, y')
```

This mirrors the induction. The base cases are $P(12)$, $P(13)$, $P(14)$, $P(15)$. The strong induction step means that $P(n-4) \implies P(n)$. In particular, if

$$n - 4 = 4x\prime + 5y\prime$$

then

$$n = 4(x\prime + 1) + 5y\prime$$

and we're done. ■

Strengthening

We can strengthen inductive hypotheses. Consider the statement that for all $n \geq 1$, we have $\sum_{i=1}^{n} i^{-2} \leq 2$. When we carry out the induction, we get $\sum_{i=1}^{k+1} i^{-2} \leq 2 + (k+1)^{-2}$, which doesn't work. So we strengthen the hypothesis, to get $\sum_{i=1}^{n} i^{-2} \leq 2 - (k+1)^{-2}$. But this doesn't work also, because the second term is hard to fit into the inductive form. A generalized approach is below.

Example 29
There exists an integral decreasing function $f(n)$ such that for all $n \geq 1$, we have $\sum_{i=1}^{n} i^{-2} \leq 2 - f(n)$.

Proof. The base case is trivial. Let $P(k) \overset{\text{def}}{\equiv} \sum_{i=1}^{k} i^{-2} \leq 2 - f(k)$. We want to prove $P(k+1)$. Then we have

$$\sum_{i=1}^{k+1} i^{-2} = \sum_{i=1}^{k} i^{-2} + \frac{1}{(k+1)^2} \leq 2 - f(k) + \frac{1}{(k+1)^2}$$

Choose $f(k+1) \leq f(k) - (k+1)^{-2}$, so

$$\sum_{i=1}^{k+1} i^{-2} \leq 2 - f(k+1)$$

One such $f(n)$ that works is $f(n) = n^{-1}$. We have

$$\frac{1}{k+1} \leq \frac{1}{k} - \frac{1}{(k+1)^2} \implies 0 \leq \frac{1}{k} - \frac{1}{k+1}$$

which is true by telescoping. Thus $f(n) = n^{-1}$ and we're done. ■

Stable Marriage Problem

Consider a town with n boys and n girls. Each girl has a ranked preference list of boys. Our goal is to match the pairings such that there do not exist a girl and a boy who prefer each other over their current partner.

We define a **pairing** as a disjoint set of n boy-girl pairs. A **rogue couple** b, g^* for a pairing S, where b and g^* prefer each other to their partners in S.

There's a stable pairing (a pairing without any rogue couples), given by the following algorithm.

Algorithm 4.1 Stable Marriage Algorithm

Input: A set of boys B and a set of girls G.
Output: A stable pairing.

```
while stable pairing does not exist do
    each boy proposes to his favorite girl on his list
    each girl rejects all but her favorite proposer, whom she puts on a string
    the rejected boys cross the rejecting girls off their lists
```

Claim. The stable marriage algorithm terminates.

Proof. All boys cross off at least one option off any list every day. The number of boys is n, and the total length of the lists is n^2. Hence the algorithm terminates in at most $n^2 + 1$ steps. ■

We have to define some metrics for such a pairing.

Lemma 30 (Improvement Lemma)
If on day t a girl g has a boy b on a string, any boy, $b\prime$ on g's string for any day $t\prime > t$ is at least as good as b.

Proof. We use induction on $t\prime$. The base case is obvious; b is at least as good as b.

The inductive step is to assume that $b\prime$ is the boy on g's string on day $t\prime$. On day $t\prime + 1$, boy $b\prime$ comes back. The girl g can choose $b\prime$, or do better with another boy $b\prime\prime$. That is, $b\prime\prime$ is better than $b\prime$ by the algorithm, so the girl does at least as well as with $b\prime$. By induction, we're done. ■

Lemma 31
Every boy is matched at the end.

Proof. Assume for the sake of contradiction, that a boy b must have been rejected n times. Every girl has been proposed to by b. By the improvement lemma, each girl has a boy on a string, and each boy is on at most one string. Since there are n girls and n boys, there are the same number of boys and girls. So b must be on some girl's string, a contradiction. Hence every boy is matched at the end. ■

Lemma 32
There is no rogue couple for the pairing formed by the traditional stable marriage algorithm.

Proof. Assume for the sake of contradiction that there is a rogue couple (b, g^*), in which b's partner is g and g^*'s partner is b^*. Since b likes g^* more than g, and g^* likes b more than b^*, we have that b proposes to g^* before proposing to g. So g^* rejected b (since he moved on). By the Improvement Lemma, g^* likes b^* better than b, a contradiction. Hence there are no rogue couples formed by the traditional stable marriage algorithm. ■

We can define a metric on the stable marriage algorithm.

Define a pairing to be x-optimal if x's partner is x's best partner in any stable pairing. Conversely, a pairing is x-pessimal if x's partner is x's worst partner in any stable pairing.

A pairing is boy-optimal if it is x optimal for all boys x, and so on.

Lemma 33
The traditional stable marriage algorithm produces a boy-optimal pairing.

Proof. Assume for the sake of contradiction that some boy b is not paired with his optimal girl g in the stable marriage pairing T. There is a stable pairing S where b and g are paired.

We use the Well-Ordering Principle. Let t be the first day a boy b gets rejected by his optimal girl g who he is paired with in the stable pairing S. Consider the boy b^* who knocks b off of g's string on day t, which implies that g prefers b^* to b. By our choice of t, b^* prefers g to his optimal girl. This implies that b^* prefers g to his partner g^* in S. This means that there is a rogue couple (b^*, g) in S, but S is stable with the couple (b, g), a contradiction. Thus the traditional stable marriage algorithm produces a boy-optimal pairing. ■

Lemma 34
The traditional stable marriage algorithm produces a boy-pessimal pairing.

Proof. Let T be a pairing produced by the stable marriage algorithm, and S be a worse stable pairing for a girl g. In T, (b, g) is a pair, and in S, (b^*, g) is a pair. In particular, g likes b^* less than she likes b. Since T is boy optimal, b likes g more than his partner in S. This produces a contradiction, since there is a rogue couple (g, b) in S, so S is not stable. Hence S does not exist. ■

5 Lecture 5

Graph theory today!

A graph is two sets, $G = (V, E)$, where V is a set of vertices and $E \subseteq V \times V$ is a subset of pairs of vertices.

A simple graph is defined as a graph where between each pair of vertices there is at most one edge; a multi-graph is a graph where this is not necessarily true.

A directed graph is a graph $G = (V, E)$ in which E is a set of ordered pairs of vertices (instead of an unordered pair).

Pick a $v \in V$. Then the neighbors of v are the vertices $u \in V$ such that $\{u, v\} \in E$.

An edge $e = \{u, v\} \in E$ is incident to vertices $u, v \in V$.

The degree of a vertex $v \in V$ is the number of incident edges to v.

For a directed graph, the in-degree of v is the number of incident edges to v in which v is the first element in the ordered pair representing the edge. The out-degree of v is analogous, where v is the second element.

Claim. The sum of the vertex degrees is twice the total number of edges. In particular,

$$\sum_{v \in V} \deg(v) = 2 \operatorname{Card}(E)$$

Proof. Each edge contributes two incidences, so $2 \operatorname{Card}(E)$ incidences are contributed in total. Also note that $\deg(v)$ is the number of incidences contributed to v. Thus the sum of the degrees of v for all $v \in V$ is the total number of incidences. Thus we get the claim. ■

Define a path in a graph to be a sequence of edges $(v_1, \ldots, v_2), (v_2, v_3), \ldots, (v_{k-1}, v_k)$. The above path has k vertices or $k - 1$ edges. A path is usually simple; it has no repeated vertices.

Define a cycle to be a path with $v_1 = v_k$. Then the length of a cycle is $k - 1$ vertices and $k - 1$ edges.

A walk is a sequence of edges with possible repeated vertices or edges.

A tour is a walk that starts and ends at the same node.

A directed path, cycle, walk, and tour are analogous for the case of directed graph.

Two vertices u and v are connected if there is a path (or walk) between u and v.

A connected graph is a graph where all pairs of vertices are connected. If one vertex v is connected to every other vertex, then the graph is connected. In particular, we have for any vertices v_1, v_2 the path $(v_1, v), (v, v_2)$.

Define the connected components of a graph as the maximal sets of connected vertices.

A Eulerian Tour is a tour that visits each edge exactly once.

Theorem 35

Any undirected graph has an Eulerian tour if and only if all vertices have even degree and the graph is connected.

Proof. First, we prove that if there is an Eulerian tour, the graph must be connected, and each vertex must have an even degree.

The Eulerian tour is connected, so the graph is connected.

On each visit to a vertex v, the tour has to enter and leave the vertex. Hence, there must be an even degree, so you can enter and exit without repetition. The tour uses two incident edges per visit, and uses all incident edges. Therefore v has even degree, so all vertices $v \in V$ have even degree.

Now, we prove that if the graph is connected and all vertices have even degree, the graph admits an Eulerian tour.

We need a small claim first:

Claim. For an arbitrary node v, we can always take a walk from v and return to v.

Proof. All vertices have even degree. If we enter, we can leave; except if we are at vertex v, in which case we are done. ■

Algorithm 5.1 Eulerian Tour Algorithm

```
Input: connected graph $G$ where each vertex has even degree
Output: Eulerian tour of $G$
  function EULERIANTOUR($G$)
      Pick a vertex $v$, take a walk from $v$ until you get back to $v$; keep walking until all the incident edges are walked over.
      Remove a cycle $C$ from $G$. The resulting graph may be disconnected. Let the components of $G$ be $G_1, \dots, G_k$. Let $v_i$ be the first vertex of $C$ that is in $G_i$. ▷ Why is there a $v_i$ in $C$? Since $G$ was connected, a vertex in $G_i$ must be incident to a vertex in $C$.
      for all $G_i \in G$ do
          $T_i$ = EULERIANTOUR($G_i$)
          Splice $T_i$ into $C$ where $v_i$ first appears in $C$.
      return C
  EULERIANTOUR($G$)
```

We will give an algorithm.

Hence, the proof is done. ■

A planar graph is a graph that can be drawn in the plane with edge crossing.

A complete graph (or clique) is a graph where every pair of vertices have an edge between them. We denote K_n as the complete graph on n vertices.

We define a bipartite graph as a graph with two disjoint sets of vertices where all the edges are between, instead of inside, the two sets. A complete bipartite graph $G = (V_1, V_2, E)$ is a graph where for each $v_1 \in V_1$ and $v_2 \in V_2$ we have $(v_1, v_2) \in E$, and no other edges exist. We denote a complete bipartite graph where $\text{Card}(V_1) = m$ and $\text{Card}(V_2) = n$ by $K_{m,n}$.

We define a face as a connected region of the plane. Note that the "outside" of a graph is also a face, even if it extends into infinity.

In a bipartite graph, all faces have even length, in the sense that each face is bordered by an even number of edges.

Theorem 36 (Euler's Formula)

Let G be a connected planar graph. Let V be the number of vertices of G, E the number of edges, and F the number of faces. Then

$$V + F = E + 2$$

We can extend Euler's formula to convex polyhedra without holes. In particular, let p be a convex polyhedra without holes and ϕ be a mapping from convex polyhedra to planar graphs. Then ϕ is an injection.

Claim. K_5 and $K_{3,3}$ are nonplanar graphs.

Proof. Consider a simple planar graph G where $V \geq 3$. Each face is adjacent to at least three edges; each edge is adjacent to at most two faces. Hence

$$3F \leq 2E$$

Plugging into Euler's formula, we have

$$3V + 2E \geq 3E + 6 \implies E \leq 3V - 6$$

From here, it's clear that K_5, which has 10 edges and 5 vertices, is nonplanar.

However, $K_{3,3}$ fulfills this formula. So we need another way to prove that it's nonplanar. Note that no cycles in $K_{3,3}$ are triangles, so there are no odd-length cycles. Every face is of length at least 4. Because all cycles are even length, the edges only go between two groups. Hence

$$4F \leq 2E$$

for any bipartite planar graph. Plugging this back into Euler's formula, we get

$$2V + E \geq 2E + 4 \implies E \leq 2V - 4$$

for bipartite planar graphs. Hence, $K_{3,3}$ is nonplanar. ■

6 Lecture 6

Euler's formula states that for a graph G with number of vertices V, faces F, and edges E,

$$V + F = E + 2$$

For different types of graphs, we can bound their quantities V, F, E by properties of the graphs.

We define a tree as a connected acyclic graph. For a tree T, we have $V = E + 1$.

We prove Euler's formula now.

Proof. We use induction on E. The base case is $E = 0$; then $V = F = 1$.

For the induction step, we use cases. If G is a tree, we plug in our values and are done. If G is not a tree, then G must have a cycle C. Remove an edge from C, which subtracts a face from the total count (since one internal face merges with the external face). This new graph has V vertices, $E - 1$ edges, and $F - 1$ faces. The graph is thus planar. By the induction hypothesis,

$$V + (F - 1) = (E - 1) + 2$$

Therefore,

$$V + F = E + 2$$

as claimed. ■

We now move onto graph coloring. Given $G = (V, E)$, a coloring of G assigns colors to vertices V where for each edge the endpoints have different colors. Note that for a graph with n vertices it's trivial to color it with n colors, so the challenge is using fewer colors than the number of vertices.

Lemma 37

Any graph with maximum degree d can be $d + 1$ colored.

Proof. We give a recursive algorithm. ■

We introduce the six color theorem.

Theorem 38

Every planar graph can be colored with six colors.

Algorithm 6.1 Coloring Algorithm

```
Input: Graph $G$ with maximum degree $d$.
Output: $d+1$ coloring of the graph.
  function COLORING($G$)
      if $V = 1$ then
          Color $v$ anything.
      Remove vertex $v$.
      COLORING($G = (V \setminus v, E)$)      ▷ Every neghbor of $v$ has at least a $d$ coloring, by induction.
      COLORING($v$)
  COLORING($G$)
```

Proof. Recall from Euler's formula that $E \le 3V - 6$ for any planar graph where $V > 2$. The total degree is $2E$, and the average degree is

$$\frac{2E}{V} \le \frac{2(3V-6)}{V} \le 6 - \frac{12}{V}$$

There exists a vertex with degree less than 6 or at most 5. We remove one such vertex; the resulting graph is planar. By induction this graph is six-colorable. Then we can color the remaining vertex with one of the missing colors (from the vertex's neighbors). ■

Claim. Connected components of vertices with two colors in a legal coloring can switch colors.

Proof. Trivial isomorphism. ■

This gives rise to the five color theorem:

Theorem 39

Every planar graph can be colored with five colors.

Proof. Start with the degree 5 vertex from before. Remove it, and recurisvely color the rest of the graph. Without loss of generality, assume that the neighbors are colored all differently (otherwise, we're done, since the neighbors take up five colors in the worst case and any less opens up a color for the vertex we removed).

Let two colors be c and c'. Then pick a neighbor n whose color is c. In n's component, switch c and c'. Then n has a possible color c to take. We're done unless there's a $c' - c$ path to another neighbor n' whose color is c'. Then we pick two more colors for c and c' and repeat this procedure. If there is the same issue with a $c - c'$ path, we know that the graph being planar implies that the two paths intersect at a vertex. Then the vertex must be two of four different colors simultaneously, a contradiction.

Thus, we can recolor one of the neighbors, which gives an available color for the center vertex. ■

We define (again) a complete graph K_n as a graph on n vertices with an edge between every two vertices. The number of edges on K_n is $\binom{n}{2}$.

We define (again) a tree as a complete graph without a cycle, or equivalently a connected graph with $V - 1$ edges, or a connected graph where any edge removal disconnects it, or a conencted graph where any edge addition creates a cycle.

We can prove the first equivalence.

Claim. The graph G is connected and has $V - 1$ edges if and only if G is connected and has no cycles.

Proof. We prove the forward directino. We begin with a lemma.

Lemma. If v has degree 1 in a connected graph G, the graph $G = (V \setminus v, E)$ is connected.

Proof. For $x \neq v, y \neq v \in V$, there is a simple path between x and y in G since G is connected, and does not use v since v is degree 1. Then $G \setminus v$ is connected. ■

We use induction on V. The base case is that $V = 1$, where there are 0 edges and no cycles.

For our induction step, we argue first that there exists a degree 1 node.

Proof. First, a graph that's connected implies that every vertex degree is at least 1. Then the sum of the degreees is $2V - 2$, and the average degree is $2 - 2/V$. Thus there exists a vertex with degree 1. ■

By the degree 1 removal lemma, $G = (V \setminus v, E)$ is connected, and it has $V - 1$ vertices and $V - 2$ edges, so by induction there's no cycle.

Now we prove the reverse direction. We walk from a vertex using untraversed edges, until we get stuck. Removing a degree 1 vertex v doesn't create a cycle (we prove that it can exist because there's at least one node where you enter but don't leave, per the definition of a walk). The new graph is connected, and removing v doesn't disconnect the graph. By induction, $G = (V \setminus v)$ has $V - 2$ edges. Then G has one more, or $V - 1$ edges. ■

We have another fact about trees:

Lemma 40

Given a tree T, there is one vertex whose removal disconnects $V/2$ nodes from each other.

Proof. Just point the edges in the other direction. ■

Complete graphs are really connected, but have lots of edges: $E = V(V-1)/2$.

Trees have few edges, but fall apart easily: $E = V - 1$.

Hypercubes are also really connected, and represent bit-strings. Let $G = (V, E)$, where $V = \{0, 1\}^d$ (where d is the dimension of the hypercube), and $E = \{(x, y) \mid x, y \text{ differ in one bit position}\}$. The hypercube has 2^d vertices; this is the same number of binary strings of length d. The hypercube also has $d2^{d-1}$ edges.

We introduce isoperimetry. For $\mathbb{R}^3$, the sphere minimizes surface area to volume. In particular, the ratio is $1/3r = \mathcal{O}(V^{-1/3})$. The graphical analog is to cut the graph into two pieces and find the ratio of edges to vertices on small side. For a tree, the ratio is $\mathcal{O}(V^{-1})$. For the hypercube, the ratio is actually $\mathcal{O}(1)$.

A formal recursive definition of a hypercube is:

- A zero-dimensional hypercube is a vertex.
- An n-dimensional hypercube is a collection of two $(n-1)$-hypercubes with edges between corresponding vertices.

Theorem 41

Any subset S of the hypercube where $\text{Card}(S) \leq \text{Card}(V)/2$ has at least $\text{Card}(S)$ edges connecting it to $V \setminus S$: we have

$$\text{Card}(E \cap S \times (V \setminus S)) \geq \text{Card}(S)$$

Note that $(S, V \setminus S)$ is a cut; and $(E \cap S \times (V \setminus S))$ is the set of cut edges.

A restatement of this theorem is that for any cut in the hypercube, the number of cut edges is at least the size of the small side.

Proof. We proceed by induction. The base case is trivial.

Now, we use the recursive definition to partition our hypercubes into two subcubes. Then we have two hypercubes connected by edges. We use casework:

Case. We can count edges inside the subcube inductively, if $\text{Card}(S) = \text{Card}(V - S)$.

Case. We can count edges inside the subcube, and across the subcubes, if $\text{Card}(S) > \text{Card}(V - S)$.

More formally, define $H_0 = (V_0, E_0)$, and $H_1 = (V_1, E_1)$, with edges E_x that connect them. Then $H = (V_0 \cup V_1, E_0 \cup E_1 \cup E_x)$, and $S = S_0 \cup S_1$.

Case. If $\text{Card}(S_0), \text{Card}(S_1) \leq \text{Card}(V)/2$, then by symmetry $\text{Card}(S_0) = \text{Card}(S_1)$, and thus $E_{tot} \geq \text{Card}(V)/2$, and we're done.

Case. If $\text{Card}(S_0) \geq \text{Card}(V_0)/2$, then $\text{Card}(S_1) \leq \text{Card}(V_1)/2$ since $\text{Card}(S) \leq \text{Card}(V)/2$. Hence in E_1 the number of edges cut is at least $\text{Card}(S_1)$.

On the other end, $\text{Card}(S_0) \geq \text{Card}(V_0)/2$ implies that $\text{Card}(V_0 \setminus S) \leq \text{Card}(V_0)/2$. Hence in E_0 the number of edges cut is at least $\text{Card}(V_0) - \text{Card}(S_0)$.

The edges in E_x connect corresponding nodes, so in E_x the number of edges cut is $\text{Card}(S_0) - \text{Card}(S_1)$.

The total edges cut, by summing up, is

$$E_{tot} \geq \text{Card}(V_0) \geq \text{Card}(V)/2$$

and we're done by induction.

Thus, the proof is complete. ■

7 Lecture 7

We begin with modular arithmetic.

Let $x, y \in \mathbb{Z}$, and $m \in \mathbb{N}$. Then x is congruent to y modulo m ($x \equiv y \pmod{m}$) if and only if $m \mid (x - y)$ or x and y have the same remainder with respect to m or $x = y + km$ for some integer k.

Addition, subtraction, and multiplication can be done with any equivalent x and y. If $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then $a + b \equiv c + d \pmod{m}$ and $ab \equiv cd \pmod{m}$. The proof is to expand.

The notation $x \pmod{m}$ or $\text{mod}(x, m)$ is the remainder r of x divided by m, such that $r \in \{0, \ldots, m-1\}$. In particular, $x \pmod{m} = x - \lfloor x/m \rfloor m$. We define the modulus as our m value.

The multiplicative inverse of x modulo m is y where $xy \equiv 1 \pmod{m}$. In modular arithmetic, 1 is still the multiplicative identity element.

Theorem 42

The number x has a multiplicative inverse modulo m if and only if $\gcd(x, m) = 1$.

Proof. For the "if" direction: we prove a claim first.

Claim. The set $S = \{0, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \pmod{m}$ if all members of S are distinct modulo m.

Proof. If members of S are not distinct, then there exists $a, b \in \{0, \ldots, m-1\}$, where $a \neq b$, where

$$ax \equiv bx \pmod{m} \implies (a-b)x \equiv 0 \pmod{m} \implies (a-b)x = km$$

for somse integer k. Since $\gcd(x, m) = 1$, the prime factorizations of m and x do not contain common primes. Hence $(a - b)$'s factorization contains all primes in m's factorization. Hence $(a - b) \geq m$, but $(a - b) \in \{0, \dots, m-1\}$, a contradiction. ■

Each of m numbers in S correspond to a different equivalence class modulo m, so one must correspond to 1 modulo m, so an inverse exists.

For the "only if" direction: let $g = \gcd(x.m)$; then $ax + bm \neq 1$ since $g(ax/g + bm/g)$ is clearly always an integer multiple of g and is thus never going to be 1. Thus, there's no modular inverse for x. ■

Claim. If $\gcd(x, m) = 1$, then the function $f(a) = ax \pmod m$ is a bijection.

Proof. The function is injective, since there is a unique pre-image (the multiplicative inverse). The function is surjective because the multiplictive inverse is clearly unique for each element of the domain. ■

We will now cover algorithms to find inverses. First, we find the greatest common divisor of x and y using the Euclidean algorithm. It relies on the claim:

Claim. We have $d \mid x$ and $d \mid y$ if and only if $d \mid y$ and $d \mid x \pmod y$.

Proof. Let $k = x/d$ and $l = y/d$. Then by computation:

$$x \pmod y = x - \lfloor x/y \rfloor y = kd - (x/y)ld = d(k - xl/y)$$

Therefore $d \mid x \pmod y$.

The reverse direction is similar, and we omit it for brevity. ■

Thus $\gcd(x, y) = \gcd(x, y \pmod x)$.

Algorithm 7.1 Euclidean Algorithm

```
Input: Two numbers $x, y \in \mathbb{N}$
Output: $\gcd(x, y)$
  function EUCLID($x, y$)
      if $y = 0$ then return $x$
      return EUCLID($y, x \pmod y$)
  EUCLID($x, y$)
```

We can prove this works by a simple strong induction argument, applying the above corollary.

For a number x, its size n in bits is $n \approx \lg x$. Then the Euclidean algorithm uses $2n$ divisions, so about $\mathcal{O}(\lg x)$, assuming $x \sim \mathcal{O}(y)$.

Fact

The first argument of the procedure decreases by at least a factor of two after two recursive calls.

Proof. We use casework.

If $y < x/2$, then the first argument is y and we're done in one recursive call.

If $y \geq x/2$, we will show that $x \pmod y \leq x/2$. Note that $x \pmod y$ is the second argument in the next recursive call and becomes the first argument in the next one after that. When $y \geq x/2$, then $\lfloor x/y \rfloor = 1$, so $x \pmod y = x - \lfloor x/y \rfloor y = x - y \leq x - x/2 = x/2$. Then we're done. ■

Now we can go about finding the inverse.

Theorem 43
For any natural x and y there are integers a and b where

$$ax + by = d \quad \text{where} \quad d = \gcd(x, y)$$

Proof. By the extended GCD theorem, when $\gcd(x, m) = 1$, then $ax + bm = 1$, so

$$ax \equiv 1 - bm \equiv 1 \pmod{m}$$

Hence a is the multiplicative inverse of $x \pmod{m}$. ■

The above, then, is the staff-endorsed Extended Euclidean algorithm.

Algorithm 7.2 Extended Euclidean Algorithm

```
Input: Two numbers $x, y \in \mathbb{N}$
Output: Integers $d, a, b$ such that $ax + by = d$, where $d = \gcd(x, y)$
  function EXTENDED_EUCLID($x, y$)
      if $y = 0$ then return $(x, 1, 0)$
      else
          $(d, a, b) \leftarrow$ EXTENDED_EUCLID($y, x \pmod{y}$)
       return $(d, b, a - \lfloor x/y \rfloor \cdot b)$
  EXTENDED_EUCLID($x, y$)
```

(However, there's a much better algorithm; check Discussion 6A or HW 03 for that. Essentially for an equation $ax + by = 1$ we can write $(m, n) = (a, b)$ and continue subtracting $\max(a, b)$ by $\min(a, b)$ and mirroring the operations in m and n until either a or b is 1, then m or n respectively is the modular inverse.)

We define a bijection as an injective and surjective function. An injective function $f : A \to B$ is that in which $f(a) = f(b) \implies a = b$. A surjective function $f : A \to B$ is that in which $f(A) = B$.

In particular, the function $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ given by $f(x) = ax \pmod{m}$ is a bijection if and only if $\gcd(a, m) = 1$. The proof is somewhat simple by expanding on the mapping and is not presented here (or in lecture), but the inuition is obvious.

Theorem 44 (Chinese Remainder Theorem)
If $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ where $\gcd(m, n) = 1$, then there is a unique solution $x \pmod{mn}$. In other words, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$.

Proof. Consider $u = n(n^{-1} \pmod{m})$. Then $u \equiv 0 \pmod{n}$ and $u \equiv 1 \pmod{m}$.

Consider $v = m(m^{-1} \pmod{n})$. Then $v \equiv 1 \pmod{m}$ and $v \equiv 0 \pmod{n}$.

Let $x = au + bv$. Then $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, due to the above congruences.

We've constructed a solution; now we show that it's unique. Assume there's another solution y. Then $(x - y) \equiv 0 \pmod{m}$ and $(x - y) \equiv 0 \pmod{n}$. Then $x - y$ is a multiple of m and n since $\gcd(m, n) = 1$. Hence $x - y \geq mn$, so $x, y \notin \{0, \ldots, mn - 1\}$, a contradiction. Thus, there's only one solution modulo mn. ■

Theorem 45 (Fermat's Little Theorem)
For prime p, and $a \not\equiv 0 \pmod{p}$, we have $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Consider $S = \{a \cdot 1, \ldots, a \cdot (p-1)\}$. They're all different modulo p since a has an inverse modulo p. Then S contains a representative of $\{1, \ldots, p-1\}$ modulo p. Then

$$(a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

Since multiplication is commutative,

$$a^{p-1}(1 \cdots (p-1)) \equiv 1 \cdots (p-1) \pmod{p}$$

Each of $2, \ldots, p-1$ has an inverse modulo p, solve to get

$$a^{p-1} \equiv 1 \pmod{p}$$

as claimed. ■

We introduce the XOR operation $a \oplus b$, where $a \oplus b$ is true if and only if one of a and b is true.

We introduce cryptography. In particular, Alice attempts to send a message m and secret key s. Then $E(m, s)$ is an encoding algorithm, and $D(m, s)$ is a decoding algorithm. One such implementation is a bitwise XOR with the secret.

We now introduce public key cryptography. Let the private key be k, and the public key be K. The message is m. Then $m = D(E(m, K), k)$. Everyone knows K, but Bob can encode, and only Alice knows the secret key k for the public key K.

It's unknown whether this is actually implementable. But we use the RSA algorithm to approximate this. Pick two large primes p and q. Let $N = pq$. Then choose e relatively prime to $(p-1)(q-1)$. Compute $d = e^{-1} \pmod{(p-1)(q-1)}$. We announce $N = pq$ and e; our public key is $K = (N, e)$.

The encoding is just take $y = m^e \pmod{N}$. The decoding is to take $y^d \pmod{N}$. This actually decodes the message, since $D(E(m)) = m^{ed} \equiv m \pmod{N}$.

We can compute $x^y \pmod{N}$ where every number is n bits by repeated squaring in $\mathcal{O}(n^3)$ time.

8 Lecture 8

Claim. Let $d \equiv e^{-1} \pmod{(p-1)(q-1)}$. We prove that

$$x^{ed} \equiv x \pmod{pq}$$

which is central to the RSA scheme.

Proof. Note that

$$ed = k(p-1)(q-1) + 1$$

By Fermat's little theorem, for prime p and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}$$

Hence

$$a^{k(p-1)} \equiv 1 \pmod{p} \implies a^{k(p-1)+1} \equiv a \pmod{p}$$

Versus

$$a^{k(p-1)(q-1)+1} \equiv a \pmod{p}$$

This is similar but not quite true. Anyways, we can exploit the isomorphism declared by the Chinese remainder theorem to get

$$e \equiv d^{-1} \pmod{(p-1)(q-1)}$$

So

$$x^{ed} \equiv x^{1+k(p-1)(q-1)} \pmod{pq}$$

Now $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$, so

$$a^{1+k(p-1)(q-1)} \equiv a\left(a^{p-1}\right)^{k(q-1)} \equiv a \pmod{p}$$

By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$ or $a = 0$. Likewise,

$$b^{1+k(p-1)(q-1)} \equiv b\left(b^{q-1}\right)^{k(p-1)} \equiv b \pmod{q}$$

By Fermat's little theorem, $b^{q-1} \equiv 1 \pmod{q}$ or $b = 0$. Hence $x^{ed} \equiv a \pmod{p}$ and $x^{ed} \equiv b \pmod{q}$. Hence by Chinese remainder theorem $x^{ed} \equiv x \pmod{pq}$. ■

Theorem 46 (Prime Number Theorem)
Let $\pi(n)$ be the number of primes less than n. For all $n \geq 17$,

$$\pi(n) \geq \frac{n}{\log(n)}$$

As a consequence, choosing a number n uniformly at random from a large interval gives an approximately $1/\log(n)$ chance of picking a prime.

To construct keys, choose two large primes p and q. Then choose an e with $\gcd(e, (p-1)(q-1)) = 1$. Then compute the inverse d of e modulo $(p-1)(q-1)$.

Breaking the scheme implies an easy factorization for n, so we're safe for now.

On the other hand, a signature scheme implies

$$E(D(C)) = (C^d)^e \equiv C \pmod{pq}$$

In some sense this is the reverse of the encryption scheme.

9 Lecture 9

We cover polynomials and error-correcting codes.

A polynomial

$$p(x) = \sum_{k=0}^{d} a_k x^k$$

is specified by coefficients $a_0, \ldots, a_d$. We define that $P(x)$ contains point (a, b) if $P(a) = b$.

A field is a set of elements with addition and multiplication with inverses. In particular, for any prime p, $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ is a field.

A real polynomial – a polynomial over $\mathbb{R}$ – is that which has real coefficients and a real domain. A polynomial over $\mathbb{F}_p$ is defined analogously.

Fact
Exactly one degree $n \leq d$ polynomial over some field $\mathbb{F}$ contains $d+1$ points.

Our objective is to share a secret among n people. Fix $k \leq n$. Any $k-1$ people will collectively know nothing; but any collection of k people with the secret will. We want to minimize the storage required, and by the above fact, we can encode the secret as the value of a polynomial $p(x) \in \mathbb{F}[x]$ at a particular point.

The method is to fix a prime p and work in $\mathbb{F}_p$. Then the secret $s \in \{0, \ldots, p-1\}$.

1. Choose $a_0 = s$, and a random $a_1, \ldots, a_{k-1}$.
2. Let $p(x) = \sum_{j=0}^{k-1} a_j x^j$ with $a_0 = s$.
3. Share i as a point $(i, P(i) \pmod{p})$, for i in the domain of p.

This gives robustness, since any k shares gives a unique polynomial p and thus a unique secret. This gives secrecy, since any $k-1$ shares gives nothing.

Example 47 (Points to Polynomial)
We work in $\mathbb{F}_5$. Then we find a line $p(x)$ such that $p(1) = 3$ and $p(2) = 4$.

Solution. We obtain the congruence system

$$\begin{array}{rcrcrl} a_1 & + & a_0 & \equiv & 3 & \pmod{5} \\ 2a_1 & + & a_0 & \equiv & 4 & \pmod{5} \end{array}$$

Subtracting, we have $a_1 \equiv 1 \pmod{5}$, and so $a_0 \equiv 2 \pmod{5}$. □

Example 48 (Points to Polynomial, Redux)
We work in $\mathbb{F}_5$. Then we find a quadratic $p(x)$ such that $p(1) = 2$, $p(2) = 4$, and $p(3) = 0$.

Solution. We obtain the congruence system

$$\begin{array}{rcrcrcrl} a_2 & + & a_1 & + & a_0 & \equiv & 2 & \pmod{5} \\ 4a_2 & + & 2a_1 & + & a_0 & \equiv & 4 & \pmod{5} \\ 4a_2 & + & 3a_1 & + & a_0 & \equiv & 0 & \pmod{5} \end{array}$$

Using linear-algebraic techniques (or just cancelling terms), we can find $a_0 = s = 4$. □

In general, given $\mathbb{F}_p$ and points $(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)$, we solve

$$\begin{array}{rcccrcrl} a_{k-1}x_1^{k-1} & + & \ldots & + & a_0 & \equiv & y_1 & \pmod{p} \\ a_{k-1}x_2^{k-1} & + & \ldots & + & a_0 & \equiv & y_2 & \pmod{p} \\ & & & \vdots & & & & \\ a_{k-1}x_k^{k-1} & + & \ldots & + & a_0 & \equiv & y_k & \pmod{p} \end{array}$$

We may solve this using row reduction over finite fields, or substitution. This method will work as long as the solutions exist and are unique. In other words, if the system is linearly independent in the vector space $\mathbb{F}_p$, we obtain a unique solution.

We provide another construction, using interpolation. Assume we're working in $\mathbb{F}_5$ and a quadratic $a_2x^2 + a_1x + a_0$ hits $(1,3), (2,4), (3,0)$. Then we can find $\Delta_1(x)$, a polynomial containing $(1,1)$, $(2,0)$, and $(3,0)$; a polynomial $\Delta_2(x)$, a polynomial containing $(1,0), (2,1), (3,0)$; and a polynomial $\Delta_3(x)$, a polynomial containing $(1,0)$, $(2,0)$, and $(3,1)$. Then $p(x) = 3\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$. Note that this process is similar to the CRT method.

As an example, $\Delta_1(x) \equiv (x-2)(x-3)(2^{-1}) \equiv (x-2)(x-3)(3) \pmod{5}$. We get 2^{-1} due to plugging in 1 and fine-tuning the result to get $\Delta_1(x) \equiv 1 \pmod{5}$. The rest are constructed in the same way.

In a more generalized way, say we're working in $\mathbb{F}$, and have a set of x-values $x_1, \ldots, x_{d+1}$, and corresponding y values. Then define

$$\Delta_j(x) = \begin{cases} 1 & \text{if} \quad x = x_j \\ 0 & \text{if} \quad x = x_j \text{ for } i \neq j \\ ? & \text{otherwise} \end{cases}$$

Given $d+1$ points, use Δ_j functions to go through the points. We have

$$p(x) = \sum_{k=1}^{d+1} y_k \Delta_k(x)$$

In fact, given points (x_1, y_1), (x_2, y_2), $\ldots$, (x_{d+1}, y_{d+1}), we define

$$\Delta_i(x) = \prod_{i \neq j}(x - x_j)\left(\prod_{i \neq j}(x_i - x_j)\right)^{-1}$$

The numerator is 0 at $x_i \neq x_j$. The inverse term makes it 1 at x_i. Then

$$p(x) = \sum_{k=1}^{d+1} y_k \prod_{k \neq j}(x - x_j)\left(\prod_{k \neq j}(x_k - x_j)\right)^{-1}$$

This is a degree d polynomial, since all Δ_i are degree d polynomials.

Claim. We now prove the uniqueness idea, that is, that at most one degree d polynomial hits $d+1$ points.

Proof. Assume, for the sake of contradiction, that two different polynomials $q(x)$ and $p(x)$ hit the same points. Then $r(x) = q(x) - p(x)$; we know $r(x)$ has $d+1$ roots, by subtracting values at each point, and is degree d. By the fundamental theorem of algebra, $r(x) = 0$, so $p(x) = q(x)$, a contradiction. ■

In general, we can write $P(x) = (x-a)Q(x) + r$; if $\deg(P(x)) = d$, then $\deg(Q(x)) = d-1$. Inducting proves the fundamental theorem of algebra.

10 Lecture 10

Error-correcting codes: erasure codes; general errors; Berlekamp-Welch algorithm; consistency of generated equations.

11 Lecture 11

Cardinality; bijective, injective, surjective maps; countable sets; rational numbers being bijective with $\mathbb{N}^2$; binary strings being bijective with $\mathbb{N}$; $\mathbb{N}[x]$ being bijective with $\mathbb{N}$; diagonalization and uncountability of $\mathbb{R}$; Cantor set being uncountable; power sets and uncountability of $\operatorname{pow}(\mathbb{N})$; continuum hypothesis.

12 Lecture 12

We begin on self-reference.

Theorem 49 (Recursion Theorem)
Given any program $P(x, y)$, we can always convert it to another program $Q(x)$ such that $Q(x) =$

$P(x, Q)$; that is, Q behaves exactly as P would if its second input is the description of the program Q.

What about if we have a program `Halt(P, I)` where `P` is a program and `I` is an input, which returns whether the program `P` halts on input `I`. Anything can be an input to a program, including other programs.

A naive implementation is to run `P` on `I` and see whether it halts, but obviously this doesn't work for arbitrarily long execution times.

Claim. There is no such function `Halt(P, I)`.

Proof. Assume for the sake of contradiction there exists a program `Halt(P, I)`. Define `Turing(P)` with the following behavior: if `Halt(P, P)` halts, then go into an infinite loop; otherwise, halt immediately. We try the function call `Turing(Turing)`.

If `Turing(Turing)` halts, then `Halts(Turing, Turing)` halts, so `Turing(Turing)` loops forever, a contradiction.

If `Turing(Turing)` loops forever, then `Halts(Turing, Turing)` does not halt, so `Turing(Turing)` halts.

Therefore, `Halt(P, I)` does not exist. ■

Proof. Any program is a fixed length string. Fixed length strings are enumerable. On any given input, the program halts or does not halt.

	P_1	P_2	P_3	$\dots$
P_1	H	H	L	$\dots$
P_2	L	L	H	$\dots$
P_3	L	H	H	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

`Halt(P_i, P_j)` is every cell, and `Turing(P_i)` is on the diagonal and is defined as the negation of `Halt`. Then we reach a diagonalization argument where `Turing` is the negation of the `P_i`th program on the `i`th input. Thus, diagonalization yields a contradiction, so `Halt(P, I)` does not exist. ■

Obviously, if we get a program for `Turing` we can construct `Halt`, or vice versa.

An easier version of the Halting Problem is to find whether a program P does a terminating action a. To solve `Halt(P, I)`, we make some P' as follows: remove all print statements from P, and find the exit points, and add statements doing the action a before them. Then call `DoesActionA(P', I)`. Then P halts if and only if P' does the action a.

Some other uncomputable problems are to tile an infinite grid with a set of finite tiles, or to solve arbitrary Diophantine equations.

We also need to cover Godel's incompleteness. We define a formal system F as a list of axioms. If in F there exists P such that $P \wedge \neg P = \textsc{True}$, then the system is inconsistent; else, it's consistent. If every statement in F has a formal proof, then the system is complete; else, it's incomplete. Godel proved that any formal system F cannot be consistent and complete.

Proof. Define the proposition $S(F)$ as the assertment that "this statement is not provable in F". If $S(F)$ is provable, then $S(F)$ so $S(F)$ is not provable, so F is inconsistent. If $S(F)$ is not provable, then $S(F)$ is true, and thus F is incomplete. ■

Now we start on probability. The product rule states that if we're picking an element from n_1 things, then an element from n_2 things, up to n_k, then the total number of possible choices is $\prod_{i=1}^{k} n_i$.

Example 50

Let S and B be finite sets. Then how many functions f map S to T?

Proof. There are $|T|$ ways to choose for $f(s_i)$ for $i \in \{1, \dots, |S|\}$, so the total number is $|S|^{|T|}$. ■

Example 51

How many polynomials of degree d exist in $\mathbb{F}_p$?

Proof. There are p ways to choose the first coefficient, p ways to choose the second, and so on, so we get p^{d+1}. ■

Proof. For each x_i for $i \in \{0, \dots, d\}$, there are p choices for $f(x_i)$. Since $d+1$ points uniquely determine a polynomial of degree d, there are p^{d+1} possible polynomials. ■

Example 52

How many 10 digit numbers exist without repeating a digit?

Proof. There are 9 ways to pick the first digit, 9 ways to pick the second digit, 8 ways to pick the third, and so on, so the total number is $9 \cdot 9!$. ■

Example 53

How many ways can we pick an ordered sample of size k from n numbers without replacement?

Proof. There are n ways for the first choice, $n-1$ ways for the second, up to $n-k+1$ ways for the last, so the total answer is $n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}$. We can show the definition of a factorial similarly. ■

Example 54

How many injective functions are there from S to S where S is a set?

Proof. Let f be an injective function from $S \to S$. Then for some fixed $i \in \{1, \dots, |S|\}$ we have that there are $|S|$ possibilities for $f(x_i)$; then there are $|S|-1$ possibilities for the next i and so on. So the total number of injective functions is $|S|!$. ■

If order doesn't matter, we count ordered objects and then divide by number of orderings.

How do we choose k objects from a pool of n objects, where we don't care about the ordering? This is just the choose function:

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

We can sum over disjoint sets to count the number of ways to do something. In particular, summing ways over mutually exclusive events gives the total number of ways. Formally, if S and T are disjoint sets, $|S \cup T| = |S| + |T|$.

We also have the principle of inclusion and exclusion, which is a generalized version of this sum rule. For any S and T, we have $|S \cup T| = |S| + |T| - |S \cap T|$.

13 Lecture 13

Three-way inclusion-exclusion can be demonstrated by a Venn diagram.

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

In general, n-way inclusion-exclusion can be given by

$$\left|\bigcup_i A_i\right| = \sum_{k=0}^{n} \sum_{\{i_1,\dots,i_k\}=I} (-1)^k \left|\bigcup_{i \in I} A_i\right|$$

Proof. Pick an element $x \in \bigcap_i A_i$. This is the maximal set that contains x. Then x is counted

$$\sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} = 1 + (1-1)^n = 1$$

■

There are $n!!$ permutations of $\{1, \dots, n\}$. Define a derangement as a permutation with no fixed point. How many derangements are there for a set? We can use inclusion-exclusion to count. Let A_i be the set of permutations where i is a fixed point, and $A_i \cap A_j$ are the permutations where i and j are fixed points. Then inclusion-exclusion states that the number of non-derangement permutations is given by the sum

$$\sum_{i=1}^{n} (-1)^{i-1} \binom{n}{i} (n-1)!$$

so the number of derangements is

$$\sum_{i=0}^{n} (-1)^{i} \binom{n}{i} (n-i)! = \sum_{i=0}^{n} (-1)^{i} \frac{n!}{i!}$$

This is the Taylor expansion of e^{-1} as $n \to \infty$. Thus, approximately $1/\mathrm{e}$ permutations are derangements.

What about sampling k items out of a pool of n items?

- Without replacement:
  - If order matters, then there's $k!\binom{n}{k}$ possibilities.
  - If order does not matter, then there's $\binom{n}{k}$ possibilities.
- With replacement:
  - If order matters, then there's n^k possibilities.
  - If order does not matter, we use Stars and Bars, so there are $\binom{n+k-1}{k-1}$ possibilities.

In general, Stars and Bars states that the number of k-tuples of positive integers that sum to n is equal to the number of $(k-1)$-element subsets of a set with $n-1$ elements, whence both of these are given by $\binom{n-1}{k-1}$; or the number of k-tuples of non-negative integers whose sum is n is equal to the number of multisets of cardinality $k-1$ taken from a set whose size is $n+1$, whence both of these are given by $\binom{n+k-1}{k-1} = \binom{n+k-1}{n}$. Basically, sampling k times from n objects with replacement and order doesn't matter yields $\binom{n+k-1}{k-1}$ possibilities.

Pascal's rule is

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

which is formed by looking at Pascal's Triangle.

Proof. There are $\binom{n+1}{k}$ size k subsets of $n+1$. If we choose the first element, then we need to choose $k-1$

more elements from the remaining n elements, which we can do in $\binom{n}{k-1}$ ways. If we do not choose the first element, then we need to choose k elements from the remaining n elements, which we can do in $\binom{n}{k}$ ways. Thus $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ as claimed. ■

We also have

$$\binom{n}{k} = \sum_{i=k-1}^{n-1} \binom{n-1}{i}$$

Proof. Consdier a size k subset where i is the first element chosen. We must choose $k-1$ elments from the $n-i$ remaining elements, which we can do in $\binom{n-i}{k-1}$ ways. We add them up to get the number of subsets of size k, which we can choose in $\binom{n}{k}$ ways. ■

We also have

$$2^n = \sum_{i=0}^{n} \binom{n}{i}$$

Proof. There are 2^n subsets of $\{1, \ldots, n\}$, since there are 2 possibilities for each element (to be in, or not in, the subset). There are also $\binom{n}{i}$ ways to choose i elements of $\{1, \ldots, n\}$. We sum over i to get the total number of subsets as 2^n again. ■

Theorem 55 (Binomial Theorem)
We have, for $n \in \mathbb{N}$,

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

Proof. We use induction on n. Obviously the hypothesis is true for $n = 1$.

One simplification we can make is $(x+y)^n = x(x+y)^{n-1} + y(x+y)^{n-1}$. Our induction hypothesis is that $(x+y)^{n-1}$ has $\binom{n-1}{k}$ terms of the form $x^{n-1-k}y^k$.

The first term gives $x^{n-k}y^k$. There are $\binom{n-1}{k-1}$ terms of the form $x^{n-1-(k-1)}y^{k-1} = x^{n-k}y^{k-1}$.

Analogously, the second term gives $x^{n-k}y^k$, so our induction means that there are $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$ terms of the form $x^{n-k}y^k$ in $(x+y)^n$, so our induction is done. ■

14 Lecture 14

We cover: definition of sample spaces (possible outcomes of an experiment), definition of probability spaces and probability; coin tosses, dice rolls, card shuffles, balls and bins (binary probability); birthday paradox; Monty Hall problem.

15 Lecture 15

Let Ω be a probability space, and A and B events in Ω. Then

- $\Pr(A) \geq 0$
- $\sum\limits_{\omega \in \Omega} \Pr(\omega) = 1$
- $A \cap B = \varnothing \implies \Pr(A \cup B) = \Pr(A) + \Pr(B)$

If $A_1, A_2, \ldots$ are mutually exclusive, then

$$\Pr\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \Pr(A_i)$$

It's clear to see that if $A \subseteq B$, then $\Pr(A) \leq \Pr(B)$.

If $A_1, \ldots, A_n$ are mutually exclusive (that is, if for all $i \neq j$ we have $A_i \cap A_j = \emptyset$), and collectively exhaustive (that is, if $\bigcup_{i=1}^{n} A_i = \Omega$), then for all events $B \subseteq \Omega$ we have

$$\Pr(B) = \sum_{i=1}^{n} \Pr(B \cap A_i)$$

For a discrete sample space Ω with equiprobable outcomes A_i, then

$$\Pr(A_i) = \frac{|A_i|}{|\Omega|}$$

Also, for an event B composed of sample points ω_i, we have

$$\Pr(B) = \sum_{\omega_i \in B} \Pr(\omega_i)$$

We see that in a probability space, the principle of inclusion-exclusion holds:

$$\Pr(A \cup B) + \Pr(A \cap B) = \Pr(A) + \Pr(B)$$

More generally,

$$\Pr\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{i_1 < \cdots < i_k} \Pr\left(\bigcap_{i \in \{i_1, \ldots, i_k\}} A_i\right)$$

Let $A, B \subseteq \Omega$ be events. Define the conditional probability of B given A as

$$\Pr(B \mid A) = \sum_{\omega \in A \cap B} \Pr(\omega \mid A) = \sum_{\omega \in A \cap B} \frac{\Pr(\omega)}{\Pr(A)} = \frac{\Pr(A \cap B)}{\Pr(B)}$$

Applying the definition of conditional probability again gives Bayes' Rule:

Theorem 56 (Bayes' Rule)
Let Ω be a sample space, with $A \subseteq \Omega$ and $B \subseteq \Omega$ events in Ω. Then

$$\Pr(A \mid B) = \frac{\Pr(B \mid A)\Pr(A)}{\Pr(B)}$$

If $\Pr(A \mid B) = \Pr(A)$, then A and B are independent events. Otherwise, they are dependent events.

16 Lecture 16

We define mututal independence in the following way. We say $A_1, \ldots, A_n$ are mutually independent if for any set S of indices such that $S \subseteq \{1, \ldots, n\}$, we have

$$\Pr\left(\bigcap_{i \in S} A_i\right) = \prod_{i \in S} \Pr(A_i)$$

For $n = 1$, an event A is only independent of itself if and only if $\Pr(A) = 0$ or $\Pr(A) = 1$.

Mutual independence always implies pairwise independence, but the reverse does not necessarily hold.

We can also have conditionally independent events. If A, B, and C are events, then if

$$\Pr(A \cap B \mid C) = \Pr(A \mid C)\Pr(B \mid C)$$

then we say that A and B are independent, conditioned on C.

We define the union-bound (also known as Boole's inequality, or subadditivity). Define $A_1, \ldots, A_n$ as a set of events, then we have from principle of inclusion/exclusion:

$$\Pr\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i=1}^{n} \Pr(A_i)$$

Proof. Define B_1 as A_1. For each $i \in \{2, \ldots, n\}$, define

$$B_i = A_i \setminus \left(\bigcup_{k=1}^{i-1} B_k\right)$$

By construction, the B_i are mututally exclusive. Hence

$$\Pr\left(\bigcup_{i=1}^{n} B_i\right) = \Pr\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \Pr(B_i)$$

Note that $B_i \subseteq A_i$ for all i, so $\Pr(B_i) \leq \Pr(A_i)$ for all i. Thus,

$$\Pr\left(\bigcup_{i=1}^{n} B_i\right) = \sum_{i=1}^{n} \Pr(B_i) \leq \sum_{i=1}^{n} \Pr(A_i) = \Pr\left(\bigcup_{i=1}^{n} A_i\right)$$

which proves the claim. ■

17 Lecture 17

Define a random variable $X(\omega) \colon \Omega \to \mathbb{R}$ as a function on a sample space Ω that maps each event $\omega \in \Omega$ to a real number $X(\omega)$. The set $\{\omega \in \Omega \mid X(\omega) = a\}$ is an event in the sample space (simply because it is a subset of Ω). This event is called $X = a$. We can talk about its probability $\Pr[X = a]$.

The distribution of a random variable X is the collection of values $\{(a, \Pr[X = a]) \mid a \in \mathscr{A}\}$, where $\mathscr{A}$ is the range of X. The collection of events $X = a$, for $a \in \mathscr{A}$, satisfy two properties:

- Any two events $X = a_1$ and $X = a_2$ with $a_1 \neq a_2$ are disjoint.
- The union of all of these events is equal to the entire sample space Ω.

The collection of events thus forms a partition of the sample space. As a consequence,

$$\sum_{a \in \mathscr{A}} \Pr[X = a] = 1$$

We define the expectation of a random variable X to be

$$\mathrm{Ex}[X] = \sum_{a \in \mathscr{A}} a\Pr[X = a]$$

Theorem 57 (Linearity of Expectation)

For any two random variables X and Y on the same probability space, we have

$$\mathrm{Ex}[X+Y] = \mathrm{Ex}[X] + \mathrm{Ex}[Y]$$

For any constant c, we have

$$\mathrm{Ex}[cX] = c\mathrm{Ex}[X]$$

Proof. Bash. Write out the expectations as summations. ■

Theorem 58 (Law of Total Expectation)
Let $A_1, \ldots, A_n$ be a partition of the sample space Ω, and X is a random variable on Ω. Then

$$\mathrm{Ex}[X] = \sum_{i=1}^{n} \Pr[A_i]\mathrm{Ex}[X \mid A_i]$$

Proof. Let $\mathscr{A}$ be the range of X.

We are given

$$\begin{aligned}\mathrm{Ex}[X] &= \sum_{x \in \mathscr{A}} x\Pr[X = x] \\ &= \sum_{x \in \mathscr{A}} x \sum_{i=1}^{n} \Pr[X = x \mid A_i]\Pr[A_i] \\ &= \sum_{i=1}^{n} \Pr[A_i] \sum_{x \in \mathscr{A}} x\Pr[X = x \mid A_i] \\ &= \sum_{i=1}^{n} \Pr[A_i]\mathrm{Ex}[X \mid A_i]\end{aligned}$$

as claimed. ■

The joint distribution for two random variables x and Y is the set $\{((a,b), \Pr[X = a, Y = b]) \mid a \in \mathscr{A}, b \in \mathscr{B}\}$, where $\mathscr{A}$ is the range of X and $\mathscr{B}$ is the range of Y. When given a joint distribution for X and Y, the distribution $\Pr[X = a]$ for X called the marginal distribution for X, and can be found by

$$\Pr[X = a] = \sum_{b \in \mathscr{B}} \Pr[X = a, Y = b]$$

In general, a joint distribution over $X_1, \ldots, X_n$ is $\Pr[X_1 = a_1, \ldots, X_n = a_n]$, where $a_i \in \mathscr{A}_i$ and $\mathscr{A}_i$ is the range of X_i. The marginal distribution for X_i is simply the distribution for $X - i$ and can be obtained by summing over all the possible values of the other variables.

Random variables $X_1, \ldots, X_n$ on the same probability space are said to be independent if the events $X_i = a_i$ are independent for all values of a_i. Equivalently, the joint distribution of independent random variables decomposes as

$$\Pr[X_1 = a_1, \ldots, X_n = a_n] = \prod_{i=1}^{n} \Pr[X_i = a_i]$$

The phrase "independent and identically distributed" denotes a set of random variables which have the same distribution and are independent. For example, the sequence of indicator functions I_i of the ith event of a random variable being a_i are independent and identically distributed.

Note that all the theorems of conditional probability hold for random variables as well.

Finally, we discuss the general form of a derived distribution. Let $g\colon \mathbb{R} \to \mathbb{R}$ be a measurable function, and let X be a random variable with range $\mathscr{A}$. Then

$$\text{Ex}[g(X)] = \sum_{a \in \mathscr{A}} g(a)\text{Pr}[X = a]$$

Note that $\text{Ex}[g(X)] \neq g(\text{Ex}[X])$ unless there exist α and β such that $g(x) = \alpha x + \beta$.

18 Lecture 18

We discuss variance and covariance. Throughout this discussion, let X be a random variable on a sample space Ω with a range $\mathscr{A}$.

Recall that

$$\text{Ex}[X] = \sum_{x \in \mathscr{A}} x\text{Pr}[X = x] \quad \text{and} \quad \text{Ex}[g(X)] = \sum_{x \in \mathscr{A}} g(x)\text{Pr}[X = x]$$

which is to say that the expected value is invariant under funcitonal representation.

Claim. For independent random variables X and Y on Ω, we have $\text{Ex}[XY] = \text{Ex}[X]\text{Ex}[Y]$.

Proof. Factorization of the joint distribution. ■

We define the variance of X as $\text{Var}[X]$ and the equation

$$\text{Var}[X] = \text{Ex}\left[|X - \text{Ex}[X]|^2\right]$$

The standard deviation is defined as $\sigma_X = \sqrt{\text{Var}[X]}$.

Claim. $\text{Var}[X] = \text{Ex}\left[X^2\right] - \text{Ex}[X]^2$.

Proof. We expand by linearity:

$$\begin{aligned}\text{Var}[X] &= \text{Ex}\left[|X - \text{Ex}[X]|^2\right] \\ &= \text{Ex}\left[X^2 - 2X\text{Ex}[X] + \text{Ex}[X]^2\right] \\ &= \text{Ex}\left[X^2\right] - 2\text{Ex}[X]^2 + \text{Ex}[X]^2 \\ &= \text{Ex}\left[X^2\right] - \text{Ex}[X]^2\end{aligned}$$

as claimed. ■

Note that $\text{Var}[X] = \text{Ex}\left[X^2\right] - \text{Ex}\left[X^2\right] = \text{Ex}[X(X-1)] + \text{Ex}[X] - \text{Ex}[X]^2$.

As an aside, we define the kth moment of X as

$$M_k(X) = \sum_{x \in \mathscr{A}} x^k \text{Pr}[X = x]$$

It's clear to see that $\text{Ex}[X] = M_1(X)$.

Claim. For independent random variables X and Y on Ω, we have

$$\text{Var}[X + Y] = \text{Var}[X] + \text{Var}[Y]$$

Proof. We have, through rote identity,

$$\begin{aligned}\text{Var}[X + Y] &= \text{Ex}\left[(X + Y)^2\right] - (\text{Ex}[X + Y])^2 \\ &= \text{Ex}\left[X^2\right] + \text{Ex}\left[Y^2\right] + 2\text{Ex}[XY] - (\text{Ex}[X] + \text{Ex}[Y])^2\end{aligned}$$

$$\begin{aligned}
&= \left(\text{Ex}\left[X^2\right] - \text{Ex}[X]^2\right) + \left(\text{Ex}\left[Y^2\right] - \text{Ex}[Y]^2\right) + 2(\text{Ex}[XY] - \text{Ex}[X]\text{Ex}[Y]) \\
&= \text{Var}[X] + \text{Var}[Y] + 2(\text{Ex}[XY] - \text{Ex}[X]\text{Ex}[Y]) \\
&= \text{Var}[X] + \text{Var}[Y] \qquad \text{(Independence)}
\end{aligned}$$

■

Now we define the covariance of two random variables.

The covariance of random variables X and Y, denoted $\text{Cov}[X, Y]$, is defined as

$$\text{Cov}[X, Y] = \text{Ex}[(X - \text{Ex}[X])(Y - \text{Ex}[Y])] = \text{Ex}[(X - \mu_X)(Y - \mu_Y)] = \text{Ex}[XY] - \text{Ex}[X]\text{Ex}[Y]$$

If X and Y are independent, then $\text{Cov}[X, Y] = 0$. However, the converse is not true. Also, it's easy to see that $\text{Cov}[X, X] = \text{Var}[X]$. Finally, for any collections of random variables $\{X_1, \ldots, X_n\}$ and $\{Y_1, \ldots, Y_m\}$ and fixed constants $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_m\}$, we have

$$\text{Cov}\left[\sum_{i=1}^{n} a_i X_i, \sum_{j=1}^{n} b_i Y_i\right] = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j \text{Cov}\left[X_i, Y_j\right]$$

For general random variables X and Y,

$$\text{Var}[X + Y] = \text{Var}[X] + \text{Var}[Y] + 2\text{Cov}[X, Y]$$

We define now the correlation between X and Y. Suppose that $\sigma_X > 0$ and $\sigma_Y > 0$. Then

$$\text{Corr}[X, Y] = \frac{\text{Cov}[X, Y]}{\sigma_X \sigma_Y}$$

This value can be shown to be between -1 and 1 no matter the values of X and Y.

Let $\mathbf{X} \colon \mathbb{R}^n \to \mathbb{R}$ be a vector random variable (a vector whose entries are scalar random variables) whose range is $\mathscr{A}$. The generalization to vector form gives us:

- $\Pr[\mathbf{X} = \mathbf{x}] = \prod_{i=1}^{n} \Pr[X_i = x_i]$
- $\text{Ex}[\mathbf{X}] = \sum_{\mathbf{x} \in \mathscr{A}} \mathbf{x} \Pr[\mathbf{X} = \mathbf{x}]$
- $\text{Ex}[g(\mathbf{X})] = \sum_{\mathbf{x} \in \mathscr{A}} g(\mathbf{x}) \Pr[\mathbf{X} = \mathbf{x}], \quad \text{Ex}[\mathbf{g}(\mathbf{X})] = \sum_{\mathbf{x} \in \mathscr{A}} \mathbf{g}(\mathbf{x}) \Pr[\mathbf{X} = \mathbf{x}]$
- $\text{Var}[\mathbf{X}] = \text{Ex}\left[(\mathbf{X} - \text{Ex}[\mathbf{X}])(\mathbf{X} - \text{Ex}[\mathbf{X}])^{\mathrm{T}}\right] = \text{Ex}\left[\mathbf{X}\mathbf{X}^{\mathrm{T}}\right] - \text{Ex}[\mathbf{X}]\text{Ex}[\mathbf{X}]^{\mathrm{T}}$
- $\text{Cov}[\mathbf{X}, \mathbf{Y}] = \text{Ex}\left[(\mathbf{X} - \text{Ex}[\mathbf{X}])(\mathbf{Y} - \text{Ex}[\mathbf{Y}])^{\mathrm{T}}\right]$
- $\text{Var}[\mathbf{X} + \mathbf{Y}] = \text{Var}[\mathbf{X}] + \text{Cov}[\mathbf{X}, \mathbf{Y}] + \text{Cov}[\mathbf{Y}, \mathbf{X}] + \text{Var}[\mathbf{Y}]$
- $\text{Corr}[\mathbf{X}]$ is defined by $[\text{Corr}[\mathbf{X}]]_{ij} = \text{Ex}\left[(X_i - \text{Ex}[X_i])(X_j - \text{Ex}\left[X_j\right])\right] / \left(\sigma_{X_i}\sigma_{X_j}\right)$

where the above are only defined if $\mathbf{X}$ and $\mathbf{Y}$ are of the same dimension.

These identities can all be derived through careful treatment of vector random variables as collections of scalar random variables.

19 Lecture 19

We discuss some distributions.

A simple yet very useful probability distribution is the Bernoulli distribution of a random variable which takes values in $\{0, 1\}$:

$$\Pr[X = i] = \begin{cases} p & \text{if } i = 1 \\ 1 - p & \text{if } i = 0 \end{cases}$$

where $0 \leq p \leq 1$. We say that X is distributed as a Bernoulli random variable with parameter p, and write

$$X \sim \text{Bernoulli}(p)$$

It's easy to see that $\text{Ex}[X] = p$. We have that the variance $\text{Var}[X] = \text{Ex}\left[X^2\right] - \text{Ex}[X]^2 = p - p^2 = p(1-p)$.

Another probability distribution is the geometric distribution, which for a random process measures the number of Bernoulli trials needed to get a success, with success probability p.

We say that X is distributed as a geometric random variable with parameter p, and write

$$X \sim \text{Geometric}(p)$$

We compute $\Pr[X = i]$. Then there are i trials, with $i - 1$ failures and 1 success. We thus have

$$\Pr[X = i] = (1-p)^{i-1}p$$

We can think of the geometric random variable as the first order interarrival time of a Bernoulli process. The process is first order because it counts until the first time a success happens.

The geometric distribution is memoryless; that is,

$$\Pr[X = x + y \mid X > x] = \Pr[X = y]$$

That is, the fact that X has failed x times does not affect anything about future outcomes.

Proof. We compute

$$\Pr[X = x + y \mid X > x] = \frac{\Pr[(X = x + y) \cap (X > x)]}{\Pr[X > x]} = \frac{(1-p)^{x+y-1}p}{\Pr[X > x]}$$

We now compute

$$\Pr[X > x] = \sum_{i=x+1}^{\infty} (1-p)^{i-1}p = (1-p)^x$$

Hence

$$\Pr[X = x + y \mid X > x] = \frac{(1-p)^{x+y-1}p}{(1-p)^x} = (1-p)^{y-1}p = \Pr[X = y]$$

as claimed. ■

We have

$$\text{Ex}[X \mid X > x] = x + \text{Ex}[X]$$

We now attempt to compute $\text{Ex}[X]$. Let A be the event of success on the first trial. By the law of total expectation, we have

$$\text{Ex}[X] = \text{Ex}[X \mid A]\Pr[A] + \text{Ex}\left[X \mid \overline{A}\right]\Pr\left[\overline{A}\right] = 1 \cdot p + (1 + \text{Ex}[X]) \cdot (1-p) \implies \text{Ex}[X] = \frac{1}{p}$$

Through a similar computation, we have

$$\text{Var}[X] = \frac{1-p}{p^2}$$

Another very useful probability distribution is the binomial distribution. Consider the random experiment of n independent trials of a process, with success probability p. Then the binomial distribution counts the number of successes.

We say that X is distributed as a binomial random variable with parameters n and p, and write

$$X \sim \text{Binomial}(n, p)$$

We compute $\Pr[X = i]$. Then there are i successes, each happening with probability p, and $n - i$ failures, each happening with probability $1 - p$. Then there are $\binom{n}{i}$ places in our sequence to put our successes, so

$$\Pr[X = i] = \binom{n}{i} p^i (1-p)^{n-i}$$

This distribution can be viewed as the distribution of a sequence of Bernoulli trials. Then

$$\text{Ex}[X] = \sum_{i=0}^{n} i \binom{n}{i} p^i (1-p)^{n-i}$$

This sum is hopeless. However, we can let $Y_1, \ldots, Y_n \sim \text{Bernoulli}(p)$, counting the success of the ith trial. We know that $\text{Ex}[Y_1] = \cdots = \text{Ex}[Y_n] = p$, and by linearity

$$X = \sum_{i=1}^{n} Y_i \implies \Pr[X] = \sum_{i=1}^{n} \Pr[Y_i] = \sum_{i=1}^{n} p = np$$

By a similar computation, we have

$$\text{Var}[X] = np(1-p)$$

Another distribution is the Poisson distribution. We say X is distributed as a Poisson random variable with parameter λ, and write

$$X \sim \text{Poisson}(\lambda)$$

The probability distribution is

$$\Pr[X = k] = \frac{\lambda^k \mathrm{e}^{-\lambda}}{k!}$$

By brute computation, we have

$$\text{Ex}[X] = \text{Var}[X] = \lambda$$

If $X_1, \ldots, X_n$ are independent Poisson random variables with parameters $\lambda_1, \ldots, \lambda_n$, we have

$$\sum_{i=1}^{n} X_i \sim \text{Poisson}\left(\sum_{i=1}^{n} \lambda_i\right)$$

If $X \sim \text{Binomial}(n, \lambda/n)$, where λ is fixed, then $\lim_{n \to \infty} X \sim \text{Poisson}(\lambda)$.

Another distribution is the uniform distribution on a set S with $|S| = n$. We say that X is distributed as a uniform random variable on S, and write

$$X \sim \text{Uniform}(S)$$

In the case that $S = [a, b]$, we write

$$X \sim \text{Uniform}(a, b)$$

We have, for $i \in S$,

$$\Pr[X = i] = \frac{1}{n}$$

and 0 otherwise. The expectation is just given by

$$\text{Ex}[X] = \sum_{i \in S} i \Pr[X = i] = \frac{1}{n} \sum_{i \in S} i$$

In the case that $S = [a, b]$, then

$$\text{Ex}[X] = \frac{a+b}{2}$$

Finally, we (re)define the indicator random variable. Let X be a random variable in a sample space with n unique sample points $\omega_1, \ldots, \omega_n$. Let $I_1, \ldots, I_n$ be random variables corresponding to the set of events $X = a$ which have the distribution

$$I_i = \begin{cases} 1 & \text{if } \omega_i \in X = a \\ 0 & \text{otherwise} \end{cases}$$

Then

$$X = \sum_{i=1}^{n} I_i \implies \text{Ex}[X] = \sum_{i=1}^{n} \text{Ex}[I_i]$$

even if the I_i are not independent (in all likelihood, they are not).

20 Lecture 20

We now attack a stereotypical problem of probability theory, the coupon collector problem.

Consider n distinct coupons, where one is randomly selected for each of a lot of boxes. Let L be the number of boxes you purchase up to, and including, the first nth distinct coupon. In other words, L describes how many boxes you purchase to get n distinct coupons in total. Define L_k to be the number of boxes it takes to get the kth unique coupon after obtaining the $k-1$th unique coupon. Each of the L_k are Bernoulli random variables with success probability $p_k = \dfrac{n-(k-1)}{n}$. Then

$$L = \sum_{i=1}^{n} L_i \implies \text{Ex}[L] = \sum_{i=1}^{n} \text{Ex}[L_i] = \sum_{i=1}^{n} \frac{n}{n-i+1} = n\left(\sum_{i=1}^{n} \frac{1}{i}\right)$$

For n large, $\text{Ex}[L] \approx \log(n) + \gamma + \frac{1}{2n}$, where γ is the Euler-Mascheroni constant.

21 Lecture 21

We discuss continuous probability distributions. In particular, we attempt to generalize our results about discrete distributions to the continuous case.

We first generalize the notion of a sample (probability) space. We firstly define a measure μ on a set X (technically a σ-algebra Σ over X), as a function with the following three properties:

- Non-negativity: for all events $E \in \Sigma$, we have $\mu(E) \geq 0$.
- Null empty set: $\mu(\emptyset) = 0$.
- For all countable collections $\{E_i\}_{i=1}^{\infty}$ of pairwise disjoint sets in Σ, we have $\mu\left(\bigcup_{k=1}^{\infty} E_k\right) = \sum_{k=1}^{\infty} \mu(E_k)$.

Then each event $E \subseteq \Sigma$ in a continuous probability space Σ is simply the analogue of a discrete event. In particular, the "size" of E is just $\mu(E)$ instead of $|E|$.

In fact, these should be ringing some bells in terms of how familiar these axioms are. This is because μ is a probability measure! So, define $\mu(E) = \Pr[x \in E]$, and to return to old notation let the probability space $\Sigma = \Omega$.

Our motivation for further particular definitions is that for any real number x, if $x \in \Omega \subseteq \mathbb{R}$ then $\mu(x) = 0$, because for every $\varepsilon > 0$ we have $x \in (x - \varepsilon, x + \varepsilon)$, so we can cover x with an arbitrarily small open interval, so it has measure 0. Thus, for every $a \in \Omega$, we have $\Pr[X = a] = 0$. This is clearly bad.

With this in mind, we try to establish a correspondance between discrete and continuous random variables. The distribution of a random variable X on Ω is given by $\Pr[a \leq X \leq b]$ for all intervals $[a, b] \subseteq \Omega$.

For this, we need to establish the notion of a probability density function $p_X(x) \colon \Omega \to \mathbb{R}$, which intuitively is the "probability of X per unit length" in the vicinity of x. This density function is not a measure, because of the lack of countable additivity, but it does have the following properties:

- Non-negativity: for all $x \in \mathbb{R}$, we have $p_X(x) \geq 0$.
- Unit measure: we have $\displaystyle\int_{x \in \Omega} p_X(x) = 1$

Then we have that the distribution of X is given by

$$\Pr[a \leq X \leq b] = \int_a^b p_X(x) \, \mathrm{d}x$$

Note that there is no necessity that $p_X(x) \leq 1$ for every x, just that it integrates to 1.

Now we connect the density $p_X(x)$ with probabilities. We look at an infinitesimally small interval $[x, x + \mathrm{d}x]$; then we have

$$\Pr[x \leq X \leq x + \mathrm{d}x] = \int_x^{x+\mathrm{d}x} p_X(z) \, \mathrm{d}z \approx \mathrm{d}p_X(x)$$

which basically affirms that $p_X(x)$ is the probability per unit length in the vicinity of x.

In this case, we know that $p_X(x)$ uniquely defines the probability distribution of X, and it is this parameter we change when we are looking at different distributions.

We now define the expectation of X over Ω with probability distribution $p_X(x)$ to be

$$\mathrm{Ex}[X] = \int_{x \in \Omega} x p_X(x) \, \mathrm{d}x$$

The variance is similarly

$$\mathrm{Var}[X] = \mathrm{Ex}\left[(X - \mathrm{Ex}[X])^2\right] = \mathrm{Ex}\left[X^2\right] - \mathrm{Ex}[X]^2 = \left(\int_{x \in \Omega} x^2 p_X(x) \, \mathrm{d}x\right) - \left(\int_{x \in \Omega} x p_X(x) \, \mathrm{d}x\right)^2$$

A joint distribution in multiple variables $X_1, \ldots, X_n$ on sample spaces $\Omega_1, \ldots, \Omega_n$ is characterized by the probability $\Pr[a_{11} \leq X_1 \leq a_{12}, \ldots, a_{n1} \leq X_n \leq a_{n2}]$. We define a joint density function $p_{X_1 \cdots X_n} \colon \bigtimes_{i=1}^n \Omega_i \to \mathbb{R}$ that satisfies

- Non-negativity: for all $x \in \bigtimes_{i=1}^n \Omega_i$, we have $p_{X_1 \cdots X_n}(x) \geq 0$.
- Unit measure: we have $\displaystyle\int_{x \in \bigtimes_{i=1}^n \Omega_i} p_{X_1 \cdots X_n}(x) \, \mathrm{d}x = 1$.

The joint distribution of $X_1, \ldots, X_n$ is given by

$$\Pr[a_{11} \leq X_1 \leq a_{12}, \ldots, a_{n1} \leq X_n \leq a_{n2}] = \int_{a_{n1}}^{a_{n2}} \cdots \int_{a_{11}}^{a_{12}} p_{X_1 \cdots X_n}(x) \, \mathrm{d}x$$

Correspondingly, $p_{X_1 \cdots X_n}(x)$ is the probability per unit n-measure.

With regards to independence, the idea is that the joint distribution factorizes. The random variables X_1, $\ldots$, X_n are independent if and only if

$$\Pr[a_{11} \leq X_1 \leq a_{12}, \ldots, a_{n1} \leq X_n \leq a_{n2}] = \prod_{i=1}^n \Pr[a_{i1} \leq X_i \leq a_{i2}]$$

From the integral definition, we are also given

$$p_{X_1 \cdots X_n}(x) = \prod_{i=1}^{n} p_{X_i}(x_i)$$

Let $X = \sum_{i=1}^{n} X_i$. Then

$$p_X(x) = p_{\sum_{i=1}^{n} X_i}(x) = (f_{X_1} * \cdots * f_{X_n})(x)$$

where

$$(f * g)(x) = \int_{-\infty}^{\infty} f(t)g(x-t)\,\mathrm{d}t$$

is the convolution of f and g.

We now discuss two continuous distributions.

For $\lambda > 0$, a continuous random variable X with density function

$$p_X(x) = \begin{cases} \lambda \mathrm{e}^{-\lambda x} & x \geq 0 \\ 0 & \text{otherwise} \end{cases}$$

is an exponential random variable with parameter λ; we say $X \sim \text{Exponential}(\lambda)$. By computing the integrals, we have $\text{Ex}[X] = \lambda^{-1}$ and $\text{Var}[X] = \lambda^{-2}$.

Note that $\text{Exponential}(\lambda) \sim \lim_{\delta \to 0} \text{Geometric}(\lambda\delta)$, which we can show by taking limits.

For $\mu \in \mathbb{R}$ and $\sigma^2 > 0$, a continuous random variable X with probability density function

$$p_X(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$$

is called a normal random variable with parameters μ and σ^2. In the special case $\mu = 0$ and $\sigma^2 = 1$, X is said to have the standard normal distribution. We write $X \sim \text{Normal}(\mu, \sigma^2)$. By taking integrals, we find that $\text{Ex}[X] = \mu$ and $\text{Var}[X] = \sigma^2$.

If X is a normal random variable with parameters μ and σ^2, then $Y = (X - \mu)/\sigma$ is a standard normal random variable. Equivalently, if Y is a standard normal random variable, then $X = \sigma Y + \mu$ has a normal distribution with parameters μ and σ. This is proved by writing the probability density and doing a change of variables.

An important property of the normal distribution is that a sum of normal random variables is also normally distributed. We begin with the simple case where the random variables are independent, and show the general case through translation.

If $X_1, \ldots, X_n$ are independent standard normal variables and $a_1, \ldots, a_n \in \mathbb{R}$, then

$$\sum_{i=1}^{n} a_i X_i \sim \text{Normal}\left(0, \sum_{i=1}^{n} a_i^2\right)$$

To show this, write out the joint distribution. Note that X is rotationally symmetric, and thus get $X \sim \sqrt{\sum_{i=1}^{n} a_i^2} X_1$ by looking at the boundary line of $\Pr[X \leq t]$. Since X_i are standard normal, we achieve the result.

Now for a really *central* theorem to statistics:

Theorem 59 (Central Limit Theorem)

Let $X_1, \ldots, X_n$ be independent and identically distributed random variables with common expectation

$\mu = \text{Ex}[X_i]$ and variance $\sigma^2 = \text{Var}[X_i]$ (both are finite). Define

$$X = \frac{\sum_{i=1}^{n}(X_i - n\mu)}{\sigma\sqrt{n}}$$

Then we have

$$\lim_{n\to\infty} X \sim \text{Normal}(0,1)$$

22 Lecture 22

We discuss three major theorems.

Theorem 60 (Markov's Inequality)
For a nonnegative random variable X with finite mean,

$$\Pr[X \geq c] \leq \frac{\text{Ex}[X]}{c}$$

Proof. Consider a constant $c \in \mathscr{A} = \text{Ran}(X)$. Then

$$\begin{aligned}\text{Ex}[X] &= \sum_{a\in\mathscr{A}} a\Pr[X = a] \\ &\leq \sum_{a\geq c} a\Pr[X = a] \\ &\leq c\sum_{a\geq c}\Pr[X = a] \\ &= c\Pr[X \geq c]\end{aligned}$$

The continuous formulation just uses the integral instead of the sum. ■

An easy generalization is

Theorem 61 (Generalized Markov's Inequality)
Let Y be a random variable with finite mean. Then for any positive constants c and r,

$$\Pr[|Y| \geq c] \leq \frac{\Pr\left[|Y|^r\right]}{c^r}$$

Proof. For $c > 0$ and $r > 0$, we have

$$|Y|^r \geq |Y|^r I(|Y| \geq c) \geq c^r I(|Y| \geq c)$$

where $I(E)$ for an event E is 1 if the event occurs and 0 otherwise. Taking expectations yields

$$\text{Ex}\left[|Y|^r\right] \geq c^r \text{Ex}[I(|Y| \geq c)] = c^r \Pr[|Y| \geq c]$$

and dividing by c^r yields the desired result. ■

We now relate the variance to the "spread" of the distribution.

Theorem 62 (Chebyshev Inequality)
For a random variable X with finite expectation $\text{Ex}[X] = \mu$ and any positive constant c, we have

$$\Pr[|X - \mu| \geq c] \leq \frac{\text{Var}[X]}{c}$$

Proof. Define $Y = X - \mu$. Then $\text{Ex}\left[Y^2\right] = \text{Var}[X]$, so apply the Generalized Markov Inequality to Y with the claimed c and $r = 2$. ■

A corollary of this is that for any random variable X with finite expectation $\text{Ex}[X] = \mu$ and finite standard deviation $\sigma = \sqrt{\text{Var}[X]}$, we have that for any constant $k > 0$,

$$\Pr[|X - \mu| \geq k\sigma] \leq \frac{1}{k^2}$$

by plugging $c = k\sigma$ into Chebyshev inequality.

If $X_1, \ldots, X_n$ are random variables with the same expectation $\text{Ex}[X_i] = \mu$ and variance $\text{Var}[X_i] = \sigma^2$, then we attempt to estimate μ by

$$\hat{\mu} = \frac{1}{n}\sum_{i=1}^{n} X_i$$

We have $\text{Ex}[\hat{\mu}] = \mu$ and $\text{Var}[\hat{\mu}] = \sigma^2/n$. Let ε be the relative error (i.e. we want to find $\hat{\mu}$ within ε of μ):

$$\Pr[|\hat{\mu} - \mu| \geq \varepsilon\mu] \leq \delta$$

Substituting $\varepsilon\mu$ for ε, we have

$$n \geq \frac{\sigma^2}{\mu^2} \cdot \frac{1}{\varepsilon^2\delta}$$

Here ε and $1 - \delta$ are the desired relative error and confidence level respectively. In practice, we use a lower bound on μ and an upper bound on σ^2 to find a suitable n.

Theorem 63 (Law of Large Numbers)
Let $X_1, X_2, \ldots,$ be a sequence of independent and identically distributed random variables with common finite expectation $\text{Ex}[X_i] = \mu$ for all i. Then their partial sums $S_n = \sum_{i=1}^{n} X_i$ satisfy

$$\lim_{n \to \infty} \Pr\left[\left|\frac{S_n}{n} - \mu\right| < \varepsilon\right] = 1$$

for every $\varepsilon > 0$.

Proof. Under the assumption that σ^2 is finite, the result is a consequence of Chebyshev inequality using the random variable S_n/n, which has expectation μ and variance σ^2/n.

Without this assumption, measure theory is required. Oops. ■

23 Lecture 23

Today, we cover Markov chains. Denote the state space of the random variables by $S = \{1, 2, \ldots, K\}$ for some finite K. The transition probability matrix $\boldsymbol{P} = [P_{ij}]_{i,j \in S}$ is a $K \times K$ matrix such that

$$P_{ij} \geq 0 \ \forall i, j \in S$$

and

$$\sum_{j\in S} P_{ij} = 1 \ \ \forall i \in S$$

Define the initial distribution as a row vector $\boldsymbol{\mu}^{(0)} = (\mu_i^{(0)} \mid i \in S)$, where

$$\mu_i^{(0)} \geq 0 \ \ \forall i \in S$$

and

$$\sum_{i\in S} \mu_i^{(0)} = 1$$

Then we define the random sequence $\{X_i\}_{i=0}^{\infty}$ by

$$\Pr[X_0 = i] = \mu_i^{(0)} \quad \text{and} \quad \Pr[X_{n+1} = j \mid X_0 = x_0, \ldots, X_{n-1} = x_{n-1}, X_n = i] = \Pr[X_{n+1} = j \mid X_n = i] = P_{ij}$$

for all $n \geq 0$ and all $x_0, \ldots, x_{n-1}, i, j \in S$. Note that so

$$\begin{aligned} \Pr\left[\bigcap_{j=1}^{n} X_j = i_j\right] &= \prod_{j=0}^{n} \Pr\left[X_j = i_j \mid \bigcap_{k=0}^{j-1} X_k = i_k\right] \\ &= \mu_{i_0}^{(0)} \prod_{j=0}^{n-1} P_{i_j i_{j+1}} \end{aligned}$$

so

$$\begin{aligned} \Pr[X_n = i_n] &= \sum_{\{i_j\}_{j=0}^{n-1} \in S} \Pr\left[\bigcap_{j=0}^{n} X_j = i_j\right] \\ &= \sum_{\{i_j\}_{j=0}^{n-1} \in S} \mu_{i_0}^{(0)} \prod_{j=0}^{n-1} P_{i_j i_{j+1}} \\ &= \left[\boldsymbol{\mu}^{(0)} \boldsymbol{P}^n\right]_{i_n} \end{aligned}$$

Thus if we denote by $\boldsymbol{\mu}^n = (\mu_i^{(n)} \mid i \in S)$ the distribution of X_n, so that $\Pr[X_n = i] = \mu_i^{(n)}$, then this derivation shows that for all $n \geq 0$ we have

$$\boldsymbol{\mu}^{(n)} = \boldsymbol{\mu}^{(0)} \boldsymbol{P}^n$$

In particular, if $\mu_i^{(0)} = 1$ for some i, then $\mu_j^{(n)} = [\boldsymbol{P}^n]_{ij} = \Pr\left[X_{n=j} \mid X_0 = i\right]$.

Consider a general finite Markov chain with transition probability matrix $\boldsymbol{P} = (P_{ij})_{i,j\in S}$ on the state space S. Let $A \subseteq S$ be a subset of states. For each $i \in S$, let $\tau(i)$ be the average number of steps until the Markov chain enters one of the states in A, given that it starts in state i. Then we have

$$\tau(i) = \begin{cases} 0 & i \in A \\ 1 + \sum_{j\in S} P_{ij}\tau(j) & \text{otherwise} \end{cases}$$

These equations are called the first step equations (FSE) for the average hitting time.

Let $\{X_j\}_{j=0}^{n}$ be a Finite Markov Chain with state space S and transition probability matrix $\boldsymbol{P}$. Further, let A, B be such that $A \subseteq S$ and $B \subseteq S$ and $A \cap B = \emptyset$. We want to determine the probability $\alpha(i)$ that, starting in state i, the Markov chain enters one of the states in A before one of the states in B. The first step equations for $\alpha(i)$ are

$$\alpha(i) = \begin{cases} \sum\limits_{j \in S} P_{ij}\alpha(j) & i \notin A \cup B \\ 1 & i \in A \\ 0 & i \in B \end{cases}$$

A distribution $\boldsymbol{\pi} = (\pi_i \mid i \in S)$ is invariant or stationary for the transition probability matrix $\boldsymbol{P}$ if it satisfies the following balance equation:

$$\boldsymbol{\pi} = \boldsymbol{\pi}\boldsymbol{P}$$

The distribution $\boldsymbol{\mu}^{(n)} = \boldsymbol{\mu}^{(0)}\boldsymbol{P}^n$ satisfies

$$\boldsymbol{\mu}^{(n)} = \boldsymbol{\mu}^{(0)} \quad \forall n \in \mathbb{N}$$

if and only if $\boldsymbol{\mu}^{(0)}$ is invariant. (The proof is by induction.)

Most Markov chains have unique invariant distributions; an exception is where $\boldsymbol{P} = \boldsymbol{I}$; there are some obvious others.

Let $I(X) = 1$ if X occurs, and 0 otherwise. We attempt to analyze how much time a Markov chain spends in state i, or the expression

$$\lim_{n \to \infty} \frac{1}{n} \sum_{m=0}^{n-1} I(X_m = i)$$

Define a Markov chain to be irreducible if it can go from every state $i \in S$ to every other state $j \in S$, possibly in multiple steps. A Markov chain is irreducible if and only if its state transition diagram is a directed graph where all nodes have paths to all other nodes.

Claim. If a Markov chain with finite state space S and transition probability matrix $\boldsymbol{P}$ is irreducible, then for any initial distribution $\boldsymbol{\mu}^{(0)}$ and for all $i \in S$, we have

$$\lim_{n \to \infty} \frac{1}{n} \sum_{m=0}^{n-1} I(X_m = i) = \pi_i$$

where $\boldsymbol{\pi} = (\pi_i \mid i \in S)$ is an invariant distribution for $\boldsymbol{P}$. Consequently, the invariant distribution exists and is unique.

Proof. The idea for a proof of this is to first define T_i as follows: assume $X_0 = i$ and let T_i be the first time after 0 that the Markov chain comes back to i. Define $\pi_i = 1/\text{Ex}[T_i]$. Over a large number n of steps, the Markov chain visits some state j and then state i about $n\pi_j P_{ji}$ times in n steps, for $j \in S$. So the total number of visits to i in n steps is the total number of visits to some j followed by a visit to i. Hence $n\pi_i = \sum\limits_{j \in S} n\pi_j P_{ji}$, so $\pi_i = \sum\limits_{j \in S} \pi_j P_{ji}$, so $\boldsymbol{\pi} = (\pi_i \mid i \in S)$ solves the balance equations. ■

We can generalize this result as follows.

Claim. Consider an irreducible Markov chain on S with transition probability matrix $\boldsymbol{P}$. For $i \in S$, define

$$d(i) = \gcd\left(n \mid n > 0, [\boldsymbol{P}^n]_{ii} = \Pr[X_n = i \mid X_0 = i] > 0\right)$$

Then $d(i)$ has the same value for all $i \in S$. If that value is 1, the Markov chain is said to be aperiodic. Otherwise, it is said to be periodic with period d. If the irreducible Markov chain is aperiodic, then for all $i \in S$,

$$\lim_{n \to \infty} \Pr[X_n = i] = \pi_i$$

where $\boldsymbol{\pi} = (\pi_i \mid i \in S)$ is the unique invariant distribution for $\boldsymbol{P}$.

This is proved similarly, with a bit more care; the proof is essentially identical for the aperiodic case.