cs70 crib

Curtis Hu

April 2023

1 Propositional Logic

Contraposition, Direct, Contradiction,

1.1 DeMorgan's Law

"Distribute and flip"

$$\neg(P \lor Q) = (\neg P \land \neg Q)$$

$$\neg(P \land Q) = (\neg P \lor \neg Q)$$

$$\neg\forall x \in Z, P(x) = \exists x \in Z, \neg P(x)$$

$$\neg\exists x \in Z, P(x) = \forall x \in Z, \neg P(x)$$

1.2 Misc

$$\exists x \forall y P(x, y) \neq \forall x \exists y P(x, y)$$

Moving the operator (it defines a new instance of y):

$$(\exists y \in Z, y < 0) \land (\exists y \in Z, y > 0) \neq \exists y \in Z(y < 0 \land y > 0)$$

It is okay here to move the operator.

$$\exists x, y \in Z, P(x) \land Q(y) = \exists x \in Z, P(x) \land \exists y \in Z, Q(y)$$

Worthwhile remembering:

$$P \Rightarrow Q \equiv \neg P \lor Q$$

2 Induction

Base case, Inductive Hypothesis, Induction Step

3 Stable Matching

1. Rogue couple is when both (M, W) prefer each other over their current partners. So look at the M's current partner, does he prefer W over her? Does W prefer M over her him? (Then they are both not satisfied with their current relationship.)

2. Improvement Lemma - the candidate's offers can only get better.

3. Job optimality in the job proposing algorithm.

4. Common counter example is a 2 × 2 case, use it.

4 Graph Theory

4.1 Tips

1. $\sum deg(v) = 2e$

2. "Five = 2 " $f + v = e + 2$, remember to count the plane as a face.

3. Eulerian Tour $\Leftrightarrow$ All degreees are even

4. Planar Graph $\rightarrow e \leq 3v - 6$

5. Non-planar $\frac{n(n-1)}{2}$

4.2 Trees

1. n vertices means n-1 edges

2. no cycles

3. connected, but removing one edge disconnects the graph

4. adding an edge creates a cycle.

5. $n - 1 - c$

4.3 Planarity

1. Complete graphs n(n-1)/2 edges

2. Planar only if no $K_5 or K_{33}$

4.4 Hypercubes

1. Have 2^n vertices (binary tree) and $n2^{n-1}$ edges

2. Bipartite

5 Modulo Arithmetics

1. $x \equiv y \mod m \Rightarrow x = am + y$
2. $10^{19} \mod 9 \Rightarrow 1^{19} \mod 9$
3. $7^{19} \mod 8 \Rightarrow (-1)^{19} \mod 8 \Rightarrow -1 \mod 8$
4. $(19 + 32) \times 11 \mod 7 \Rightarrow (5 + 4) \times 4 \mod 7$
5. Inverses. Division doesn't work in mod space, but that doesn't mean an inverse can't exist. For small numbers, just guess and check the inverse.
6. The formal way of finding an inverse (useful in Lagrangian interpolation and CRT) is using Extended Euclidean Algorithm (GCD).

5.1 FLT

Assume p is prime (or p and a are coprime):

$$a^p \equiv a \mod p$$

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

5.2 EGCD

First decompose:

$$\begin{aligned} gcd(129, 7) &= 1 \\ 129 &= 7(18) + 3 \\ 7 &= 3(2) + 1 \\ 7 - 3(2) &= 1 \end{aligned}$$

Then substitute the remainders from the first part.

$$\begin{aligned} 7 - (129 - 7(18))(2) &= 1 \\ 7 - (129(2) - 7(36)) &= 1 \\ 129(-2) + 7(37) &= 1 \end{aligned}$$

6 RSA

Often times, p and q are very large primes 512 bit each. The encryption key is often key is a small value relatively prime to $(p-1)(q-1)$. The decryption key is where the real magic comes. It is the inverse of e, which is unique to our choice of p and q.

Information lives in the modspace of pq (cannot be greater than pq -1 or less than 0 without losing information)

1. (N,e), N = pq
2. RoT: all the e and q are derived in modspace (p-1)(q-1)
3. $e \mod (p-1)(q-1)$
4. $d = e^{-1} \mod (p-1)(q-1)$
5. Important property: $ed = 1 \mod (p-1)(q-1)$
6. $x^e \mod pq$ is our encrypted message
7. $(x^e)^d = x^{ed} \mod pq$ is decrypted

Works due to FLT and CRT:

$$\begin{align}
ed &\equiv 1 \mod (p-1)(q-1) \tag{1}\\
ed &= k(p-1)(q-1)+1 \tag{2}\\
x^{ed} &\equiv x \mod pq \tag{3}\\
x^{ed} &= kpq + x \tag{4}\\
x^{ed} &= x^{k(p-1)(q-1)+1} \tag{5}\\
x^{k(p-1)(q-1)+1} &\equiv x \mod pq \tag{6}\\
(x^{k(q-1)})^{(p-1)} x &\equiv x \mod p \tag{7}\\
x &\equiv x \mod p \tag{8}\\
(x^{k(p-1)})^{(q-1)} x &\equiv x \mod q \tag{9}\\
x &\equiv x \mod q \tag{10}\\
x &\equiv x \mod pq \tag{11}\\
\tag{12}
\end{align}$$

7 Error Correction

Your packets will come in pairs $(index, message)$ where the message is in modspace of a prime.

7.1 Erasure Errors

Simply put, you need d points unique identify a $d-1$ degree polynomial. Hence, you need to send enough correct packets so that after the maximal number of erasure errors, we still have d points.

7.1.1 Lagrange Interpolation

1. For each point, you create an expression that is zero for every other index, but for its own index returns the message at that index.

2. Plug into the form where p is the prime modspace the messages were already sent with. It is done here for index 1:

   $$\Delta_1 = \frac{(x-b_0)(x-b_2)(x-b_3)}{(1-b_0)(1-b_2)(1-b_3)} \mod p$$

   Notice that the top and bottom are the same but you plugin the index as x for the denominator. Notice that for every other index the expression results in 0. For its own index, the expression results in 1.

   However division is not permitted in modspace, so replace with the inverse of the value of the denominator. That way the expression still returns 1.

3. The resulting polynomial is:

   $$m_0\Delta_0 + m_1\Delta_1 + m_2\Delta_2 + m_3\Delta_3 \mod p$$

7.1.2 Polynomial Interpolation

We take a different approach here. On the receiving side, we know the message length. Hence we know the degree polynomial we need to create. With this information we plugin the values and solve for the coefficients in a matrix. For values (1, 8), (2, 3), (3, 2) in modspace 11:

$$a_2(1)^2 + a_1(1) + a_0 = 8$$

$$a_2(2)^2 + a_1(2) + a_0 = 3$$

$$a_2(3)^2 + a_1(3) + a_0 = 2$$

Solve for the coefficients and you'll receive the polynomial. This is guaranteed since .

7.2 General Errors

The idea is that we create a new expression that accounts for possible errors by zero-ing them out. Note that $Q(x)$ has $n+k$ coefficients and $E(x)$ has k coefficients.

$$P(x)E(x) = rE(x)$$

$$Q(x) = r_xE(x)$$

$$E(x) = (x-b_0)(x-b_1)... = x^k + b_{k-1}x^{k-1} + ... + b_0$$

Remember to fully recreate the message you need $n+2k$ total packets.

1. With the received packets, write out $Q(x) = r_xE(x)$ using polynomial interpolation. So it would be in the form $a_2(1)^2 + a_1(1) + a_0 = 2(1^1 + b_0)$ if k = 1 and message is 2 length. Note that doing so means you know the original message length.

2. Solve with Gaussian elimination or LU decomposition. With the coefficients, you can just use $\frac{Q(x)}{E(x)}$

8 Counting

8.1 Tricks

1. n^k Tree model
2. $n!$ Choices
3. $\frac{n!}{(n-k)!}$
4. $\frac{n!}{(n-k)!k!}$
5. bins and balls
6. stars and bars

8.2 Stars and Bars

Combination: 4 buckets and 17 balls.

$$C(stars + bars, bars)$$

Sometimes, its easier to think of them as bins instead of bars and stars.

8.3 PIE

Tricks: let one be determined and count the rest divide by the permutations of a subset if order doesn't matter for those

For a uniform sample space, you could find the probabilty of something with (num of favorable)/(total num of outcomes)

9 Countability and Computability

9.1 Countability

1. Injective "unique inputs yields unique outputs" (one-to-one) or more formally, $\forall x, y(f(x) = f(y) \Rightarrow x = y$
2. Surjective "hits everying in the output range." More formally, $\forall b \in B(\exists a \in A, f(a) = b)$
3. Bijection both unique inputs yields unique outputs and hits everything in the output range.

9.1.1 Countable Tricks

1. Set if countable if bijection exists between it and a the natural numbers.
2. $\mathbb{Z}, \mathbb{N}, \mathbb{Q}$ are countable.
3. $\mathbb{Q}^c, \mathbb{R}$ are uncountable.
4. Any subset of a countable set is countable. Like naturals or integers.
5. Finite set is countable
6. Countable union of countable sets is countable.
7. $\mathbb{Q}$ is countably infinite on an interval.
8. The powerset of a countably infinite set is uncountable.
9. $\mathbb{Q} \to \mathbb{N}$ using spiral over all a xy plane (every possible pair of integers)
10. Reals are uncountable (proof via diagonalization)

9.2 Computability

1. The Halting Problem is uncomputable

$$Halt(P, x) = \begin{cases} Halts & \textbf{if on P(x) halts} \\ Loops & \textbf{if on P(x) loops forever} \end{cases}$$

Asking if something is computable basically asks if I can run this without running the entire program. Consider the only two scenarios: it is finite and terminates or it enters a while loop. Can your question be determined in both situations (without having to run the while loop indefinitely).

Imagine that your program is a txt file of some really long length and is a vast sea of unknown.

1. Does it halt in n steps? Computable, just the run the program for n steps
2. Does it touch the memory location n? To know this for any program with certainty, we'd need to run the whole file or at least until we find out. This reduces to the Halting Problem.

Let's create a program called Turing that will cause a contradiction

$$Turing(P) = \begin{cases} Loop & \textbf{if on Halt(P, P) Halts} \\ Halt & \textbf{otherwise} \end{cases}$$

This yields a contradiction

$$Turing(Turing)$$

This shows us that Halt(P, x) is really unreliable because if not, we'd be able to build upon it over and over again.

9.2.1 Godel's Incompleteness Theorem

Is arithmetic complete and consistent? Godel's argument that it is incomplete. This means there are statements in arithmetic that are true, but you could never prove them. Here's Godel's argument.

10 Probability

10.1 Symmetry

Given a set of trials the principle of symmetry states that the probabiliyt of each trial is independent of the other trials. Without additional information.

10.2 Independence

1. $P(A \cap B) = P(A)P(B) \Leftrightarrow Independent$
2. $Ind \Rightarrow E[XY] = E[X]E[Y]$
3. $P(A|B) = P(A)$
4. $Ind \Rightarrow Cov(X, Y) = 0$
5. $Ind \Rightarrow Var(X + Y) = Var(X) + Var(Y)$
6. Two sets can only be same set, disjoint, independent, have some overlap.

10.3 LTP

$$P(A) = \sum P(A \cap B_i)$$

10.4 Conditional Probablity

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Someitmes you'll need to write $P(B)$ using TPR.

10.5 Expectation Rules

1. Regardless of independence. $E[X + Y] = E[X] + E[Y]$
2. $E[X] = \sum xP(X = x)$
3. $E[g(X)] = \sum g(X)P(X = x)$
4. $E[\sum \alpha_i X_i] = \sum \alpha_i E[X_i]$

5. Conditional: $E[X|Y] = \sum xPr(X = x|Y)$
6. LIE: $E[X] = E[E[X|Y]]$
7. LTE: $E(X) = \sum E[X|Y = y]Pr(Y = y)$

10.6 Covariance Rules

1. cov(X,Y) = E[XY] - E[X]E[Y]
2. cov(X,Y) = cov(Y,X)
3. cov(A + B,Y) = cov(A,Y) + cov(B,Y)

10.7 Variance Rules

1. $Var(X) = E[(X - \mu)^2] = E[X^2] - \mu^2$
2. $Var(X + a) = Var(X)$
3. $Var(aX) = a^2 Var(X)$
4. $Var(X + Y) = Var(X) + Var(Y) + 2Cov(X, Y)$

10.8 Chebychevs Inequality

Just finds lower/upper bounds on continuous distributions.

1. $P(X \geq a) \leq \frac{E[X]}{a}$ Markov's Inequality
2. $P(|X - \mu| \geq a) \leq \frac{Var(X)}{a^2}$ Main Form
3. Alternate Form: $P(|X - \mu| \leq a) \geq 1 - \frac{Var(X)}{a^2}$
4. Alternate Form: $P(|X - \mu| \leq k\sigma) \geq 1 - \frac{1}{k^2}$

$$P(|X - \mu| \geq a) = P((X - \mu)^2 \geq a^2) \leq \frac{E[(X - \mu)^2]}{a^2}$$

10.9 LLN

As $n \to \infty$ the estimated mean approaches the true mean.

$$Pr(|M_n - \mu| \geq a) \to 0$$

11 Distributions

11.1 RoT

1. $Ind \Rightarrow Cov = 0$

   $Independent \Rightarrow E[XY] = E[X]E[Y]$

   $Cov(X,Y) = E[XY] - E[X]E[Y]$

2. $Var(X+Y) = Var(X) + Var(Y) + 2Cov(X,Y)$

11.2 Bernoulli

A single H/T flip with probability of heads of p

1. $P[X = i] = p$
2. $E[X] = p$
3. $Var[X] = p(1-p)$

11.3 Binomial

A number of heads/tails flips

1. $X \sim Bin(n,p)$
2. $P[X = i] = \binom{n}{i}(1-p)^{n-i}p^i$
3. HHT, HTH, HHT Order matters
4. $E[X] = np$
5. $Var[X] = np(1-p)$

11.4 Geometric

Number of biased coin flips until first heads.

1. $P[X = i] = (1-p)^{i-1}p$
2. $E[X] = \frac{1}{p}$
3. $Var(X) = \frac{1-p}{p^2}$ (Don't really need to know)
4. "Memoryless Property"

11.5 Poisson

Number of successes per unit of time (rare). Like a skewed normal distribution.

1. $P[X = i] = \frac{\lambda^i}{i!}e^{-\lambda}$
2. $E[X] = \lambda$
3. $Var(X) = \lambda^2$
4. Adding RV. $X \sim Poisson(\lambda), Y \sim Poisson(\mu) \Rightarrow X+Y \sim Poisson(\lambda+\mu)$

11.6 Negative Binomial Distribution

Sum of geometrically distributed random variables. Number of times until ith success

1. parameters: p is probabilty of success for a given, independent trial. t is the number of random variables to add.
2. $P[X = k] = \binom{t-1}{k-1}(1-p)^{t-k}p^k$
3. $E[X] = \frac{t}{p}$
4. $Var[X] = \frac{t(1-p)}{p^2}$

11.7 Uniform

1. $E[X] = l/2$
2. $$f(x) = \begin{cases} 0 & x < 0 \\ \frac{1}{l} & 0 \le x \le l \\ 0 & x > l \end{cases}$$
3. $$F(x) = \begin{cases} 0 & x < 0 \\ \frac{x}{l} & 0 \le x \le l \\ 1 & x > l \end{cases}$$

11.8 Exponential

Continous analog of Geometric. How long until first instance of something.

1. $X \sim Exp(\lambda)$
2. $$f(x) = \begin{cases} \lambda e^{-\lambda x} & x \ge 0 \\ 0 & otherwise \end{cases}$$

3. $$F(x) = \begin{cases} 0 & x < 0 \\ 1 - e^{-\lambda x} & x \geq 0 \end{cases}$$

4. $E[X] = \frac{1}{\lambda}$

5. $Var[X] = \frac{1}{\lambda^2}$

6. ”Memoryless” property

7. Minimum of exponential RV. $E_i \sim Exp(\lambda_i)$ then $min(E_1, ..., E_k) \sim Exp(\sum_i \lambda_i)$

8. Property $aX \sim Exp(\lambda/a)$

11.9 Normal

1. $X \sim N(\mu, \sigma^2)$

2. Don’t remember this:
$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

3. $E[X] = \mu$

4. $Var[X] = \sigma^2$

5. Sum of independent random variables. $N_i \sim N(\mu_i, \sigma_i^2)$ where each N_i is independent, then $\sum_i N_i \sim N(\sum_i \mu_i, \sum_i \sigma_i^2)$

6. Standardizing.

   With $X \sim N(\mu, \sigma^2)$ we can create a new RV $Z = \frac{X-\mu}{\sigma} \sim N(0, 1)$

   Similarly, using a standardized RV $Z \sim N(0, 1)$ we can create a new RV $X = Z\sigma + \mu \sim N(\mu, \sigma^2)$

7. ”Linearity” For independent standard normal RVs: $X \sim N(0, 1) and Y \sim N(0, 1)$, then $Z = aX + bY \sim N(0, a^2 + b^2)$

8. ”Linearity” Let $X \sim N(\mu_x, \sigma_x^2), Y \sim N(\mu_y, \sigma_y^2)$ be independent normal random variables. Then $Z = aX + bY \sim N(a\mu_x, +b\mu_y, a^2\sigma_x^2 + b^2\sigma_y^2)$

11.10 Gamma Distribution

Continous analog of negative binomial. For a sum of exponentially distributed RV, what are the number of times until the ith success

1. $E[X] = \frac{k}{\lambda}$

2. $Var[X] = \frac{k}{\lambda^2}$

12 Continous Probability

1. Summations are integrals.
2. PDF is continous while PMF is discrete
3. Draw the distribution and integrate over the area of interest
4. $E[X] = \int_{-\infty}^{\infty} xf(x)dx$
5. $Var[X] = \int_{-\infty}^{\infty} x^2 f(x)dx - E[X]^2$
6. Joint probability is probability spread out on a plane. (Such as a normal bell) $1 = \int \int f(x, y)dydx$. However, we find the amount of probability in a region of area.
7. Independence is again $f(x, y) = f_x(x)f_y(y)$