Practice Final Solutions

Problem 1 [True or False] (10 points)

T $\forall x \exists y(P(x) \Rightarrow Q(y)) \equiv \neg\exists x \forall y(P(x) \wedge \neg Q(y))$

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

F $\exists x \exists y \exists z \forall d(P(d) \implies d = x \vee d = y \vee d = z)$ means that there are at most 4 distinct numbers that satisfy $P(x)$.

This means that there are at most 3 distinct numbers that satisfy $P(x)$.

T For any prime number p, $\gcd(p, 2^{p-1} - 1) = p$.

This follows from Fermat's little theorem: $2^{p-1} = 1 \bmod p$ for any prime p.

F $3^{16} = 2 \mod 5$

Using repeated squaring you can calculate $3^{16} = 1 \mod 5$.

F The security of RSA is based on Fermat's little theorem.

The security of RSA is based on the assumption that factoring is hard.

F When Alice and Bob want to communicate using RSA, Alice uses her public key (N, e) to encode messages and Bob uses his own private key d to decode those messages.

Alice needs to use Bob's public key to encode messages that she wants to send to him.

F Secret sharing does not work, if the key is the value of the polynomial at $x = 2$ (as opposed to the secret being $s = P(0)$).

The exact same reasoning applies regardless of the value x we pick to have $s = P(x)$.

T To recover from k general errors, it suffices to transmit $n + 2k + 1$ messages when using the Berlekamp-Welch method.

In fact it is enough to transmit $n + 2k$ messages, but $n + 2k + 1$ also allows us to recover from the errors.

T The number of ways to marry n boys with n girls is $n!$.

It is the number of permutations of the n boys.

F When doing inference in order to de-noise a signal, our end goal is to estimate with absolute certainty the exact value of the signal at any given time-point.

We can never estimate the exact value of the signal with probability 1; rather we are interested in its posterior distribution.

Problem 2 [Induction] (15 points)

Prove that $7^{2n} - 48n - 1$ is divisible by 2304 for every natural number n.

Solution

Let $P(n) : 2304 | f(n)$ where $f(n) = 7^{2n} - 48n - 1$.

- Firstly, $f(1) = 7^{2 \cdot 1} - 48 \cdot 1 - 1 = 0$ and $2304|0$. So $P(1)$ is true.
- Now assume $P(k)$ is true, for some natural number k, i.e.

$$2304 | f(k)$$

We now deduce $P(k+1)$.

$$\begin{aligned} f(k+1) &= 7^{2(k+1)} - 48(k+1) - 1 \\ &= 7^{2k} \cdot 7^2 - 48(k+1) - 1 \\ &= (7^{2k} - 48k - 1) \cdot 49 + (48k+1) \cdot 49 - 48(k+1) - 1 \\ &= 49 \cdot f(k) + (48k+1) \cdot 49 - 48(k+1) - 1 \\ &= 49 \cdot f(k) + (49-1) \cdot 48k + 49 - 48 - 1 \\ &= 49 \cdot f(k) + 2304k \\ &\equiv 0 \mod 2304, \text{ since } 2304 | f(k) \text{ by the inductive assumption} \end{aligned}$$

So $P(k+1)$ is true, if $P(k)$ is true.

Problem 3 [Stable Marriage] (20 points)

1. Consider an instance of the Stable Marriage problem in which the men are $\{1, 2, 3, 4\}$, the women are $\{A, B, C, D\}$, and the preference lists are

Men (1-4)					Women (A-D)				
1:	A	B	D	C	A:	2	3	4	1
2:	C	B	A	D	B:	1	4	2	3
3:	D	C	B	A	C:	1	4	2	3
4:	D	C	A	B	D:	1	3	2	4

   Use the traditional marriage algorithm to find the male-optimal pairing.

Day	1	2	3
A:	**1**	**1**	**1**
B:			**2**
C:	**2**	2, **4**	**4**
D:	**3**, 4	**3**	**3**

   So, the male-optimal pairing is $(A, 1), (B, 2), (C, 4), (D, 3)$.

2. Given n men and n women, what is the minimum number of stable pairings that must exist for any set of preferences? Justify your answer by describing an instance.

   The minimal number of stable pairings is 1. This happens when the male-optimal and female-optimal pairings are the same. An example of this is when man 1 and woman A have each other on the top of their list, man 2 and woman B have each other on the top of their list, and so on. The only stable pairing in this instance is $(1, A), (2, B), \ldots$.

3. We saw in the homework that it was possible for a pairing to be stable even if there was a pair (M, W) such that M was W's least favorite man and W was M's least favorite woman. What is the maximum number of couples with this property (each member is paired with their least favored partner) can there be in any stable pairing? Justify your answer.

   The maximum number is 1; suppose that this is not true - that there is a situation where we have a stable paring that has at least two such couples - call them $(1, A)$ and $(2, B)$. In this situation we know that 1 and A have each other on the bottom on their preference lists, and 2 and B have each other on the bottom of their preference lists. So, from this we know that 1 must prefer B over A, and 2 must prefer 1 over 2. Therefore, $(1, B)$ is a rogue couple, which contradicts the fact that the pairing was stable. Thus, we have a contradiction, and there can be at most one such couple with this property in any stable pairing.

Problem 4 [Modular Arithmetic] (10 points)

1. How many polynomials of degree d are there over arithmetic mod q (GF(q))? (Any degree $d' < d$ polynomial is also a degree d polynomial.)

   Assuming $q \geq d+1$, there are q^{d+1} unique polynomials of degree d over (GF(q)).

   Given d and q with $q \geq d+1$, we can fix $d+1$ different values in GF(q), $\{x_1, x_2, ..., x_{d+1}\}$. Then there are q^{d+1} ways to assign y-values $\{y_1, y_2, ..., y_{d+1}\}$ so that the points $(x_1, y_1), (y_1, y_2), ..., (x_{d+1}, y_{d+1})$ lie on a degree d polynomial over GF(q). Each such assignment specifies a unique degree d polynomial; furthermore, as we proved in class, every degree d polynomial can be specified in this way.

2. Consider the following process for generating random degree d polynomials over GF(q). ($q > d$.) Generate $d+1$ point-value pairs, $\{(0, r_0), (1, r_1)..., (d, r_d)\}$ where each r_i is an integer chosen independently and uniformly at random from $\{0, \ldots, q-1\}$. What is the probability that the polynomial is $x^d + x^{d-1} ... + x + 1$(i.e., the polynomial whose coefficients are all 1)?

   Working over GF(q), there are q^{d+1} possible assignments of values $(r_0, ..., r_d)$ to $d+1$ point-value pairs, and, since each r_i is chosen independently and uniformly from $\{0, \ldots, q-1\}$, each of these assignments is equally likely. The polynomial $p(x) = x^d + x^{d-1} ... + x + 1$ corresponds to exactly one of these q^{d+1} assignments of values to $d+1$ point-value pairs: $r_0 = p(0), r_1 = p(1), ..., r_d = p(d)$.

   Thus the probability is $\frac{1}{q^{d+1}}$ that the polynomial whose coefficients are all 1 is chosen.

Problem 5 [Graphs] (10 points)

If G is a graph on $n \geq 4$ vertices and $deg(v) \geq n-2$ for every vertex v, then G contains an n-cycle.

Base case: G has 4 vertices, all of them have degree 2 or greater. Consider one vertex v_1, which is connected to at least two other vertices v_2 and v_3. Both v_2 and v_3 have to have at least one other edge coming out – this leads to two cases: v_1, v_2, v_3 form a 3-cycle (i.e. a triangle) or v_2 and v_3 are both connected to v_4. The latter possibility is a 4-cycle since we have formed a square. So we're left with the case that v_1, v_2, v_3 is a triangle. But v_4 also has at least two edges coming out of it. We may rotate the triangle, so that without loss v_4 is connected to v_2 and v_3. In this case again we have a square: $v_1v_2v_4v_3v_1$.

v1 must be connected to at least 2 other vertices since it has at least degree 2. And since v1 is connected to v2 and v3 (by edges), v2 and v3 need to have at least one edge that is connected to them, so that they have more than 1 edge connected to them (want 2 edges coming into a vertex for even degree of 2). Then either a triangle or a square can exist since there can be a triangle of deg 2 on each vertex or square with deg 2 on each vertex. But you want an n-cycle, and that means that you would want to have a cycle of length 4. To take care of the case where you have a triangle, which a 3 cycle instead of a 4 cycle that's desired, you know that since you have 4 vertices, each one must have even degree for a square to work. You know that v4, the fourth vertex, must also have even degree and would therefore have at least 2 edges coming out of it. Apparently, you can rotate the triangle to form a square, since a square is made up of two triangles.

Induction hypothesis: Assume that for some fixed $n \geq 4$, any graph G on n vertices with $deg(v) \geq n-2$ for every vertex must have an n-cycle.

Induction step: Consider a graph G on $n+1$ vertices, with $deg(v) \geq (n+1)-2 = n-1$ for every vertex. We want to show G has an $(n+1)$-cycle.

Pick a vertex w of G and now consider the remaining vertices and the edges between them. They form a graph G' on n vertices. Furthermore, for each vertex v of G', we have deleted at most one edge (the edge between v and w, if it existed), so we have reduced the degree of v by at most one. So that means $deg_{G'}(v) \geq deg_G(v) - 1 \geq (n-1) - 1 = n-2$. So G' is a graph on n vertices with all vertices having degree at least $n-2$. By the induction hypothesis, G' has an n-cycle, so let's list it out clockwise: $v_1v_2 \ldots v_nv_1$. Now back to considering w. We know $deg(w) \geq n-1$, so there is at most one of the v_i that is not connected with w. Suppose without loss that v_1 is not connected with w. Since $n \geq 4$, vertices v_2 and v_3 are distinct from v_1. But w is connected with v_2 and v_3, so we create an n-cycle as follows: $v_1v_2wv_3 \ldots v_nv_1$. So G has an n-cycle.

Induction Step where you want to show that G has a (n+1) cycle: Pick any vertex w of G, and consider the remaining vertices and the edges between these remaining vertices, these for a graph G' on n vertices (b/c currently not considering 1 vertex). Now for G', thinking about every vertex v of it, we have deleted at most one edge (b/t one of the v and w if the edge existed), so we've reduced the degree of v by at most one. Then degG'(v) at least >= degG -1(v) so that's at least (n-1) - 1 = n - 2 now, so G' is a graph on n vertices with all vertices having degree at least n-2. By induction hypothesis, G' has an n-cycle. Now consider w again, and you know that deg(w) >= n-1 by the proposition given. Suppose v1 is not connected with w, since n>= 4, vertices v2 and v3 are distinct from v1, but w is connected with v2 and v3, so cre es an n-cycle.

Problem 6 [Probability 1] (15 points)

Suppose Alice encodes 40 packets of data into 100 packets to transmit to Bob, using the polynomial-based error correction code discussed in class.

Suppose that each transmitted packet is dropped independently with probability 0.5.

1. What is the exact probability that Bob can recover the data? (You do not have to evaluate the expression.)
   The encoding scheme can tolerate up to 60 dropped packets. Let X be the number of dropped packets; $X \sim Bin(100, 0.5)$. Bob can recover the message when $X \leq 60$. Thus, the probability he can recover the message is

$$\Pr[X \leq 60] \;=\; \sum_{i=0}^{60} \binom{100}{i} \cdot 0.5^i \cdot 0.5^{100-i} \;=\; \sum_{i=0}^{60} \binom{100}{i} \cdot 0.5^{100}.$$

2. Compute a positive lower bound on the probability that Bob will be able to recover the data.
   Since $\mathrm{E}[X] = 50$, by Markov's inequality, $\Pr[X \geq 61] \leq \frac{50}{61} \approx 0.18$. Thus, Bob can recover the message with probability at least $\frac{11}{61} \approx 0.82$.
   Since $\mathrm{Var}(X) = 100 \cdot 0.5 \cdot 0.5 = 25$, we have from Chebyshev's inequality:

$$\Pr[X - 50 \geq 11] \;\leq\; \Pr[|X - 50| \geq 11] \;\leq\; \frac{25}{121} \;\approx\; 0.21.$$

   Thus, Bob can recover the message with probability at least 0.79.

3. Using the Central-Limit Theorem, give an approximation to the probability that Bob can recover the data. You will need the fact $\Pr[Y > 2] = 0.023$, where Y follows the standard normal distribution. How do you compare this approximation to the lower bound you derived in part 2?
   We approximate X as a normal distribution $N(50, 25)$. Let Y be a standard normal. Than $\Pr[X > 60] = \Pr[Y > \frac{60-50}{5}] = \Pr[Y > 2] = 0.023$. Thus, the probability that Bob can recover the message is about 0.967. This is a significantly higher probability than the bounds obtained from either Markov or Chebyshev.

Problem 7 [Probability 2] (20 points)

(a) State and prove Bayes' rule for events, from the definition of conditional probability.

Recall that the definition of conditional probability is

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

So, we have:

$$\begin{aligned} \Pr[A|B] &= \frac{\Pr[A \cap B]}{\Pr[B]} \\ &= \frac{\Pr[B|A]\Pr[A]}{\Pr[B]} \end{aligned}$$

which is Bayes' rule.

Once again we are in the situation of gambling with a dishonest friend. Your friend has three coins; one comes up Heads with probability $\frac{1}{4}$, one comes up Heads with probability $\frac{1}{2}$, and one comes up Heads with probability $\frac{3}{4}$. You decide to play a game - he picks a coin randomly from his stash of three coins - you then guess what coin he picked. If you guess correctly, you win two dollars; otherwise you lose one dollar.

(b) Is this game fair? - i.e., do you expect to lose money, win money, or break even?

We pick the right coin with probability $\frac{1}{3}$, and we pick the wrong coin with probability $\frac{2}{3}$; so, the amount of money we expect to gain is:

$$\frac{1}{3} \cdot 2 + \frac{2}{3} \cdot (-1) = 0$$

So, we expect to break even.

You still seem wary, so your friend offers to help you out; for the coin that he selects, he will flip it until it comes up Heads. You can then make your guess.

(c) Your friend flips and the first Heads appears in the third flip. What coin would you guess? Justify your answer with a calculation. (Hint: You may not need to compute all the probabilities to figure out what the optimal guess is.)

Let C_i be the event that your friend picked the i^{th} coin; let X_1 be the number of flips until the first heads appeared; so, given C_1, we know that $X_1 \sim Geo\left(\frac{1}{4}\right)$; given C_2, we know that $X_1 \sim Geo\left(\frac{1}{2}\right)$; given C_3, we know that $X_1 \sim Geo\left(\frac{3}{4}\right)$ In order to guess, we need to calculate $\Pr[C_i|X_1 = 3]$ for $i = 1, 2, 3$.

$$\begin{aligned} \Pr[C_1|X_1 = 3] &= \frac{\Pr[C_1]}{\Pr[X_1 = 3]} \cdot \Pr[X_1 = 3|C_1] \\ &= \frac{\Pr[C_1]}{\Pr[X_1 = 3]} \cdot \left(\frac{3}{4}\right)^2 \left(\frac{1}{4}\right) \\ &= \frac{\Pr[C_1]}{\Pr[X_1 = 3]} \cdot \frac{9}{64} \end{aligned}$$

$$\begin{aligned}
\Pr[C_2|X_1=3] &= \frac{\Pr[C_2]}{\Pr[X_1=3]} \cdot \Pr[X_1=3|C_2] \\
&= \frac{\Pr[C_2]}{\Pr[X_1=3]} \cdot \left(\frac{1}{2}\right)^2 \left(\frac{1}{2}\right) \\
&= \frac{\Pr[C_2]}{\Pr[X_1=3]} \cdot \frac{8}{64}
\end{aligned}$$

$$\begin{aligned}
\Pr[C_3|X_1=3] &= \frac{\Pr[C_3]}{\Pr[X_1=3]} \cdot \Pr[X_1=3|C_3] \\
&= \frac{\Pr[C_3]}{\Pr[X_1=3]} \cdot \left(\frac{1}{4}\right)^2 \left(\frac{3}{4}\right) \\
&= \frac{\Pr[C_3]}{\Pr[X_1=3]} \cdot \frac{3}{64}
\end{aligned}$$

Comparing these three probabilities, we know that $\Pr[X_1 = 3]$ is the same through all of them, and also $\Pr[C_1] = \Pr[C_2] = \Pr[C_3]$; so we just look at the last term and see that it is most likely that we have the first coin. So we guess that it is the first coin.

You still don't like this arrangement - so you convince your friend to flip the same coin he selected again until it comes up Heads.

(d) Your friend flips and the first Heads now appears on the second flip. What coin would you now guess? Justify your answer with a calculation. (Hint: You may not need to compute all the probabilities to figure out what the optimal guess is.)

In this problem we use the same logic as above, although we replace the marginal probabilities with the new conditional probabilities; define X_2 to be the number of coins we flip until we see the first heads; we need to calculate $\Pr[C_i|X_2 = 2, X_1 = 3]$ for $i = 1, 2, 3$.

$$\begin{aligned}
\Pr[C_1|X_2=2, X_1=3] &= \frac{\Pr[C_1|X_1=3]\Pr[X_2=2|C_1, X_1=3]}{\Pr[X_2=2|X_1=3]} \\
&= \frac{\Pr[X_1=3]}{\Pr[X_1=3, X_2=2]} \Pr[X_2=2|C_1]\Pr[C_1|X_1=3] \\
&= \frac{\Pr[X_1=3]}{\Pr[X_1=3, X_2=2]} \cdot \frac{\Pr[C_1]}{\Pr[X_1=3]} \cdot \frac{9}{64} \cdot \frac{3}{4} \cdot \frac{1}{4}
\end{aligned}$$

$$\begin{aligned}
\Pr[C_2|X_1=3, X_2=2] &= \frac{\Pr[C_2|X_1=3]\Pr[X_2=2|C_2, X_1=3]}{\Pr[X_2=2|X_1=3]} \\
&= \frac{\Pr[X_1=3]}{\Pr[X_1=3, X_2=2]} \Pr[X_2=2|C_2]\Pr[C_2|X_1=3] \\
&= \frac{\Pr[X_1=3]}{\Pr[X_1=3, X_2=2]} \cdot \frac{\Pr[C_2]}{\Pr[X_1=3]} \cdot \frac{8}{64} \cdot \frac{2}{4} \cdot \frac{2}{4}
\end{aligned}$$

$$\begin{aligned}
\Pr[C_3|X_1=3,X_2=2] &= \frac{\Pr[C_3|X_1=3]\Pr[X_2=2|C_3,X_1=3]}{\Pr[X_2=2|X_1=3]} \\
&= \frac{\Pr[X_1=3]}{\Pr[X_1=3,X_2=2]}\Pr[X_2=2|C_3]\Pr[C_3|X_1=3] \\
&= \frac{\Pr[X_1=3]}{\Pr[X_1=3,X_2=2]}\cdot\frac{\Pr[C_3]}{\Pr[X_1=3]}\cdot\frac{3}{64}\cdot\frac{1}{4}\cdot\frac{3}{4}
\end{aligned}$$

Once again, all of the leading terms are the same through the three equations, so we just need to consider the trailing term. So, we see that the second probability is the largest, and so we would now guess that the coin is the second coin.

Problem 8 [Continuous Probability] (10 points)

The time that your mother arrives home in the evening is uniformly distributed in $[6, 8]$ (in p.m. times). Once your mother arrives home, she will call your father and he will arrive at a time uniformly distributed between the arrival time of your mother and 8 p.m.

Your friend claims that the arrival time of your father is also uniformly distributed in $[6, 8]$, and you want to see if he is correct.

1. Let X and Y be the arrival times of your mother and father respectively. Compute the joint probability density function $f_{X,Y}(x, y)$. (Make sure you specify the range of x and y for which the density is non-zero.) Are X and Y independent?

$$f_X(x) = \begin{cases} \frac{1}{2} & 6 < x < 8 \\ 0 & \text{else} \end{cases}$$

$$f_{Y|X}(y|x) = \begin{cases} \frac{1}{8-x} & x < y < 8 \\ 0 & \text{else} \end{cases}$$

So

$$f_{X,Y}(x, y) = f_X(x) f_{Y|X}(y|x) = \begin{cases} \frac{1}{2}\frac{1}{8-x} & 6 < x < 8, x < y < 8 \\ 0 & \text{else} \end{cases}$$

X and Y are not independent: $f_{Y|X}(y|x) = 0 \neq f_Y(y)$ for $y < x$.

2. Compute the probability density function of Y. Is your friend correct?

(You may find the following fact useful: $\int_c^d \frac{1}{a-x} dx = \ln \frac{a-c}{a-d}, \qquad c < d < a$)

For $y \in [6, 8]$,

$$\begin{aligned} f_Y(y) &= \int_{-\infty}^{\infty} f(x, y) dx \\ &= \int_6^y \frac{1}{2(8-x)} dx \\ &= \frac{1}{2} \ln \frac{2}{8-y}, \end{aligned}$$

and $f_Y(y) = 0$ otherwise.

Since $f_Y(y)$ is not constant, Y is not uniformly distributed in $[6, 8]$.