Asli's Midterm 1 Review Answers

1. Implication & Logic

(a) A and $\neg A$ cannot simultaneously be true, so the proposition is false for all models. Hence, not valid; not satisfiable; unsatisfiable.

(b) $A = B = C = F$ makes this proposition true. $A = T, B = C = F$ makes this proposition false. So, it is true for some models and false for some models. Hence, not valid; satisfiable; not unsatisfiable.

(c) Rewrite the proposition as $(B \vee \neg A) \vee (A \vee \neg B)$ to see it is true for all models. Hence, valid; satisfiable; not unsatisfiable.

Remark: These problems can also be answered using full truth tables, but as shown above, this can be avoided in each case.

2. Map Coloring

(a) Call the two colors 0 and 1. For each $i = 1, \ldots, n$, let X_i be true iff country j is colored with color 1. Then for a 2-coloring to be feasible, any two adjacent countries i and j must have different colors, so one of X_i and X_j is true and one is false. Hence, the following proposition is satisfiable if and only if there is a feasible 2-coloring;

$$P \equiv \bigwedge_{(i,j):\, C_i,\, C_j \text{ adjacent}} (X_i \wedge \neg X_j) \vee (\neg X_i \wedge X_j)$$

To convert it to CNF, we use the distributivity to get

$$\begin{aligned} P &\equiv \bigwedge_{(i,j):\, C_i,\, C_j \text{ adjacent}} (X_i \vee \neg X_i) \wedge (X_i \vee X_j) \wedge (\neg X_j \vee \neg X_i)\, (\neg X_j \vee X_j) \\ &\equiv \bigwedge_{(i,j):\, C_i,\, C_j \text{ adjacent}} (X_i \vee X_j) \wedge (\neg X_j \vee \neg X_i) \end{aligned}$$

(b) We may, without loss of generality, assume country C_1 is colored with color 1, so $X_1 = T$. We wish to see if C_2 must then also be always colored with color 1. In other words, we wish to test if $X_1 \wedge P \implies X_2$ is valid, or, equivalently, if $\neg(X_1 \wedge P \implies X_2)$ is unsatisfiable. We have:

$$\begin{aligned} \neg(X_1 \wedge P \implies X_2) &\equiv \neg(\neg(X_1 \wedge P) \vee X_2) \\ &\equiv X_1 \wedge P \wedge \neg X_2 \end{aligned}$$

which is in CNF since P is in CNF. This CNF expression is unsatisfiable if and only if C_1 and C_2 must have the same color in any feasible 2-coloring.

Remark: For part (a), many people tried to construct variables X_{ij} which were true iff countries i and j are adjacent. But these are not *variables*! For any given map, the adjacency relations are fixed; they determine the structure of the logical constraints on the colors.

Asli's Midterm 1 Review Answers

3. Induction:

In the inductive step, the proof for $P(n+1)$ appeals to $P(n)$ and $P(n-1)$, which fails for $n+1=2$ because $P(n-1)$ is $P(0)$ which is unproved (and false).

Remark: For part (a), many people essentially pointed out that $5n-5$ is not equal to 0 for all n, or found nonexistent errors in the first line of the inductive step. The inductive step is perfectly correct given P(n) and P(n-1).

4.

If $13x = 5 \pmod{46}$, what is x? (Short answer.) Compute the inverse of $13 \pmod{46}$ using iterative Euclid.

$$13(0)+46(1)=46$$
$$13(1)+46(0)=13$$
$$13(-3)+46(1)=7$$
$$13(4)+46(-1)=6$$
$$13(-7)+46(2)=1$$

This gives an inverse of -7, which says $x=-35=11 \pmod{46}$. Checking, we get $(13)(11)=143=(3)\times 46+5=5 \pmod{46}$.

5.

What is the maximum number of solutions for x in the range $\{0,\dots,N-1\}$ for any equation of the form $ax=b \pmod{N}$, when $gcd(a,N)=d$? (Short answer: an expression possibly involving N, a, b, and/or d.)

The maximum number of solutions is d.

If b is a multiple of d, we are looking for solutions to $ax=b+kN$ for integer k. But all of them are multiples of d, so we are looking for solutions to $a'x=b' \pmod{N'}$.

There is one solution to this equation modulo N', since $gcd(a',N)=1$. Any solution of the form $x+iN'$ remains a solution, and there are d values of i where x remains in the range $\{0,\dots,N-1\}$.

6.

Given an n-vertex tree, Bob added 10 edges to it, then Alice removed 5 edges and the resulting graph has 3 connected components. How many edges must be removed to remove all cycles in the resulting graph? (An expression that may contain n.)

7

The problem is asking you to make each component into a tree. The components should have n_1-1, n_2-1 and n_3-1 edges each or a total of $n-3$ edges. The total number of edges after Bob and Alice did their work was $n-1+10-5=n+4$, thus one needs to remove 7 edges to ensure there are no cycles.

Asli's Midterm 1 Review Answers

7. Quantifiers

   (a) $(\forall n \in \mathbb{N})(P(n))$
   D - If P is a statement which is always true, this proposition holds. If P is sometimes false, this statement will not hold.

   (b) $(P(0) \wedge P(1)) \rightarrow ((\forall n \in \mathbb{N})(n \geq 1 \rightarrow P(n)))$
   D - If P is a statement which is always true, this proposition could hold. If P is sometimes false, this statement will not hold. The base cases are insufficient to show the proposition holds for any values of n except powers of 2.

   (c) $((\forall n \in \mathbb{N})(n \text{ is odd} \rightarrow P(n))) \rightarrow ((\forall n \in \mathbb{N})(n \geq 1 \rightarrow P(n)))$
   T - If $P(n)$ holds for all odd n, it must hold for all $n \in \mathbb{N}$, because every n is either itself odd or a power of 2 multiplied by an odd number.

   (d) $(\forall n \in \mathbb{N})(P(2n))$
   D - If P is a statement which is always true for even n, this proposition holds. If P is sometimes false, this statement will not hold.

8. Short Answers

   (a) What is $3^{240} \pmod{77}$?
   Answer: $3^{240} = (3^{60})^4 = 1^4 = 1 \pmod{77}$

   The second step follows from $7^{(p-1)(q-1)} = 1 \pmod{77}$.

   (b) What is $3^{16} * 3^{-1} \mod 7$? (Hint: the multiplicative inverse of 3 is 5 modulo 7 and repeated squaring.)
   Answer: $(3^{16}) * 3^{-1} = ((3^2)^2)^2 * 5 = 6 \pmod{7}$

   (c) Given an RSA scheme for large primes p and q where $q < p < 2q$ we can set $e = p$ and get a valid construction. (True or False.)
   Answer: True. p is co-prime to $(p-1)(q-1)$ in this case, as $p-1$ cannot contain q as a factor, and vice versa, and both p and q are prime.

   (d) What is d for RSA scheme with $(N = 143, e = 11)$?
   Answer: We have $N = 11(13) = 143$, we want $11^{-1} \pmod{(10)(12)}$ which is 11.

Asli's Midterm 1 Review Answers

9.

(a) How many different degree $\leq d$ polynomials modulo p contain d points; $(x_1, y_1), \ldots, (x_d, y_d)$. (Assume that $p > d$.)

Answer: Choosing a y value for one more point makes the polynomial unique; thus, since there are only p possible y-values for this point, the number of polynomials is at most p.

(b) What is the maximum number of times that a degree 4 polynomial, $P(x)$, and a degree 2 polynomial, $Q(x)$, can intersect? (That is, what is the maximum number of x-values where $P(x) = Q(x)$.)

Answer: At most $d = 4$. The difference polynomial, $P(x) - Q(x) = 0$, has to be 0 at the intersection points, and has at most d zeros.

(c) What is the minimum modulus that could be used to send the message $3, 4, 3$ through a channel that drops 3 packets?

Answer: One needs to send 6 packets. Thus, the modulus should be at least 7, which is prime and allows one to have more than 6 different x-values for your points.

(d) What is the polynomial that encodes the message $3, 3, 0$ modulo 7. (Use the x values $0, 1, 2$ in your encoding.)

Answer: $P(x) = 2x^2 - 2x + 3$

Solve a linear system. It works out pretty ok, but takes a minute or two.

(e) What is the error polynomial for Berlekamp-Welsh for a message $\pmod{11}$ where errors appeared at $x = 2$ and $x = 4$?

Answer: $(x-2)(x-4) = x^2 + 5x + 8 \pmod{11}$

(f) We are working modulo seven, $\pmod 7$, in this problem. We have polynomials

$$\begin{array}{lll} p_1(1) = 3 & p_1(2) = 0 & p_1(3) = 0 \\ p_2(1) = 1 & p_2(2) = 1 & p_2(3) = 0 \\ p_3(1) = 0 & p_3(2) = 0 & p_3(3) = 1 \end{array}$$

Describe a polynomial $p(x)$ where $p(1) = 5, p(2) = 3$ and $p(3) = 1$ in terms of polynomials $p_1(x), p_2(x)$, and $p_3(x)$. (Remember this is all $\pmod 7$.)

Answer: $3p_1(x) + 3p_2(x) + p_3(x)$.

Start with $5(5p_1(x)) + 3(p_2(x) - 5p_1(x)) + p_3(x)$ where each term comes from an appropriate Δ functions.

10.

1. $(\neg P \implies R) \wedge (\neg P \implies \neg R) \equiv P$
   Answer: True. This is proof by contradiction.
2. $\forall x \in \mathbb{N}, (P(x) \wedge (\exists y \in \mathbb{N}, Q(x,y)) \equiv \forall y \in \mathbb{N}, \exists x \in \mathbb{N}, P(x) \wedge Q(x,y)$.
   Answer: False. $P(x)$ is True. $Q(x,y)$ is $y > x$.
3. $(\neg P(0) \wedge \forall n \in \mathbb{N}, (P(n) \implies P(n-1))) \equiv \forall n \in \mathbb{N}, \neg P(n)$
   Answer: True. This is the well ordering principle on $\neg P(n)$.
4. $\forall x, ((P(x) \implies Q(x)) \wedge Q(x)) \equiv \forall x, P(x)$
   Answer: False. If $Q(x)$ is true that implies nothing about $P(x)$.
5. $P \vee Q \equiv \neg P \implies Q$ **Answer:** True. This is the logical equivalence of $P \implies Q$ and $\neg P \vee Q$.

11.

Use induction to prove that $1 + \frac{1}{2} + \cdots (\frac{1}{2})^n \leq 2$? (Hint: strengthen the statement.)
Answer: Statement: $1 + \frac{1}{2} + \cdots (\frac{1}{2})^n = 2 - (\frac{1}{2})^n$
Base Case: $n = 0$. Plug in and we get $1 = 2 - (\frac{1}{2})^0$.

Induction Step:

$$\begin{aligned} 1 + \cdots + (\frac{1}{2})^{n+1} &= 2 - (\frac{1}{2})^n + (\frac{1}{2})^{n+1} \\ &= 2 - ((\frac{1}{2})^n - (\frac{1}{2})^{n+1}) \\ &= 2 - (\frac{1}{2})^{n+1} \end{aligned}$$

12.

Consider a directed graph where every pair of vertices u and v are connected by a single directed arc either from u to v or from v to u. Show that every vertex has a directed path of length at most two to **the vertex with maximum in-degree.** Note that this is quite similar to a homework problem but asks for a more specific answer. (Hint: Our solution doesn't require induction.)

Answer: The total in-degree is the number of arcs which is $n(n-1)/2$ and thus the vertex v with maximum in-degree must have in-degree d at least $(n-1)/2$.

Thus, these d vertices has a path of length 1 to v. The other vertices, of which there are $n-1-d$, have in-degree at most d and thus out-degree at least $n-1-d$, thus each must have an arc to one of the d vertices directly connected to v.

13.

For all $n \geq 3$, the complete graph on n vertices, K_n has more edges than the d-dimensional hypercube for $d = n$. (True or False)

False

This is just an exercise in definitions. The complete graph has $n(n-1)/2$ edges where the hypercube has $n2^{n-1}$ edges. For $n \geq 3$, $2^{n-1} \geq (n-1)/2$.

The complete graph with n vertices where p is an odd prime can have all its edges covered with x Rudrata cycles: a cycle where each vertex appears exactly once. What is the number, x, of such cycles in a cover? (Answer should be an expression that depends on n.)

$\frac{p-1}{2}$.

Each cycle removes degree 2 from each node. As the degree is $p-1$, we obtain a total of $\frac{p-1}{2}$. This is if it can be done disjointly.

14.

(a) Prove or disprove that for integers a, b, if $a+b \geq 1016$ that either a is at least 508 or b is at least 508.

Proof: by contraposition. Contrapositive: if both a and b are less than 508 than $a+b < 1016$.

Proof of contrapositive: $a+b < 508+508 > 1016$. □

Asli's Midterm 1 Review Answers

15.

RSA, CRT and Inverses. 20 points.

Show work as asked. Place final answers in boxes, but provide justification where asked, and we may evaluate work outside the box for partial credit.

1. Given an RSA public key pair $(N, e = 3)$, somehow you obtain d. Give an efficient algorithm to find p and q? (Hint: e is 3.)

   Answer: $de - 1 = k(p-1)(q-1)$ for $k = 1$ or $k = 2$ or $k = 3$. One can try each to obtain $Y = (p-1)(q-1)$ in at least one of the cases. Then, you have $Y = pq - p - q + 1$ and $pq = N$. Plugging in N/q for p and multiplying through by q into the first equation yields $Yq = Nq - N - q^2 + q$. This is a quadratic equation which one can solve to figure out q. This is similar to the homework problem.

16.

1. What is $2^{24} \pmod{35}$?

   Answer: $1 \pmod{35}$. RSA says $a^{(p-1)(q-1)} = 1 \pmod{35}$.
2. What is the $x \pmod{105}$ where $x = 1 \pmod 3$, $x = 0 \pmod 5$ and $x = 0 \pmod 7$?

   Answer: 70. $5 \times 7 \times (2^{-1} \pmod 3) \pmod{105}$ or 70.
3. How many numbers in $\{0, \ldots, 104\}$ are relatively prime to 105?

   Answer: 48. $(p-1)(q-1)(r-1) = (4)(6)(2)$.
4. What is $2^{49} \pmod{105}$?

   Answer: 2. The modulus is pqr for $p = 5$,$q = 7$, $r = 3$. We know from homework that $a^{(p-1)(q-1)(r-1)} = 1 \pmod{105}$. Here $(p-1)(q-1)(r-1) = 48$, so we multiply 1 by 2.
5. What is the multiplicative inverse of 3 modulo 37?

   Answer: 25. One can use extended GCD, or see that $3 \times 12 = 36 = -1 \pmod 37$, thus multiplying by -12 or 25 gives 1. This is clear in a low depth egcd as well.

17.

1. (Short Answer.) Give a number y modulo 35, where $y = 0 \pmod 5$ and $y = 1 \pmod 7$.
   Answer: 15. This is $5 \times (5^{-1} \pmod 7) \pmod{35}$ or one can enumerate the multiples of 5 and check.
2. (Short Answer.) Give a number y modulo 35, where $y = 1 \pmod 5$ and $y = 0 \pmod 7$.
   Answer: 21. Ths is $7 \times (7^{-1} \pmod 5) \pmod{35}$ or one can enumerate the multiples of 7 and check.
3. (Short Answer)Give a number y modulo 35, where $y = 4 \pmod 5$ and $y = 3 \pmod 7$.
   Answer: 24, which is $((4 \times 21) + (3 \times 15)) \pmod{35}$.
4. (True/False) The public key d is relatively prime to $(p-1)(q-1)$.
   Answer: True. Since d has an inverse (e) modulo $(p-1)(q-1)$, it must be that $gcd(d,(p-1)(q-1)) = 1$.
5. Consider an RSA scheme where $p = 23, q = 5$ and $e = 3$. What is d?
   Answer: $(p-1)(q-1) = 88$.

$$\begin{aligned}
3(0) + (1)(88) &= 88 \\
3(1) + (0)(88) &= 3 \\
3(-29) + (1)(88) &= 1
\end{aligned}$$

   Thus $d = -29 = 59$.

Asli's Midterm 1 Review Answers

18. True False

    (a) A proposition and its contrapositive cannot both be true.
    Circle one: **True** **False**
    Answer: False. A proposition is always equivalent to its contrapositive.

    (b) The proposition $(A \wedge B) \vee (\neg A \wedge B) \vee \neg B$ can never be false.
    Circle one: **True** **False**
    Answer: True. The proposition can be simplified to $B \vee \neg B$, which is always true.

    (c) The hypercube graph always has an Eulerian tour.
    Circle one: **True** **False**
    Answer: False. To have an Eulerian tour the degree of each vertex must be even. For the hypercube graph this is only true when the dimension is even.

    (d) If $f: A \to B$ is an injective (1-1) function, then there exists a surjective (onto) function $g: B \to A$.
    Circle one: **True** **False**
    Answer: True. We can construct g by assigning $g(b) = a$ if there exists $a \in A$ with $f(a) = b$, and assigning $g(b)$ arbitrarily otherwise.

    (e) If $\gcd(a,b) = d$, then a has no factor larger than d.
    Circle one: **True** **False**
    Answer: False. $\gcd(a,b) = d$ means a and b have no common factor larger than d, but a itself can still have factors larger than d.

    (f) In RSA with modulus $n = 91$ and encryption power $e = 5$, the decryption power is $d = 73$ because $de = 365 \equiv 1 \bmod 91$.
    Circle one: **True** **False**
    Answer: False. We need $de \equiv 1 \bmod (p-1)(q-1)$. In this case $p = 7$, $q = 13$, so $(p-1)(q-1) = 72$, and we need $d = 29$ so that $de = 145 \equiv 1 \bmod 72$.

    (g) If the multiplicative inverse $a^{-1} \bmod p$ exists for all $a \in \{1, \ldots, p-1\}$, then p is a prime.
    Circle one: **True** **False**
    Answer: True. The condition implies p is relatively prime to all $a \in \{1, \ldots, p-1\}$, which means p is a prime.

    (h) For any $d \in \mathbb{N}$, the set of polynomials of degree d with integer coefficients is countable.
    Circle one: **True** **False**
    Answer: True. The set of polynomials of degree d with integer coefficients is in bijection to $\mathbb{Z}^{d+1}$, which is countable.