FOCS HW 11 for Day 12 Solution Set

I. Formal Proofs

Use the rules of inference from class (reprinted below) to construct formal, numbered proofs of the following:

1. Assuming p -> q and p -> r, prove p -> (q AND r)

Note that there are many correct answers. Here is one.

1. p -> q	assumption
2. ~p v q	1, conditional (first form on sheet)
3. p -> r	assumption
4. ~p v r	3, conditional (first form)
5. (~p v q) ^ (~p v r)	2, 4, conjunction
6. ~p v (q ^ r)	5, distributive (second form, backwards)
7. p -> (q ^ r)	6, conditional (first form, bkwds)

QED

2. Assuming p -> (q OR r) and p -> (q OR NOT r), prove p -> q

1. p -> (q v r)	assumption
2. ~p v (q v r)	1, conditional (first form)
3. (~p v q) v r	2, associative (2d form, bkwds)
4. p -> (q v ~r)	assumption
5. ~p v (q v ~r)	4, conditional (first form)
6. (~p v q) v ~r	5, associative (2d form, bkwds)
7. ((~p v q) v r) ^ ((~p v q) v ~r)	3, 6, conjunction
8. (~p v q) v (r ^ ~r)	7, distributive (2d form, bkwds)
9. (~p v q) v F	8, negation (second form)
10. ~p v q	9, identity (second form)
8. p -> q	10, conditional (first form, bkwds)

QED

II. Truth tables

Use a truth table to show the equivalence of the assumptions and conclusion from problem 1, above: Assuming p -> q and p -> r, prove p -> (q AND r)

First, we make a truth table for each of the three formulae (the two assumptions and the thing to be proved. I added a column for q^r to make the final column's logic clearer.

p	q	r	**p -> q**	**p -> r**	q ^ r	**p -> (q ^ r)**
F	F	F	T	T	F	T
F	F	T	T	T	F	T
F	T	F	T	T	F	T
F	T	T	T	T	T	T
T	F	F	F	F	F	F
T	F	T	F	T	F	F
T	T	F	T	F	F	F
T	T	T	T	T	T	T

Next, we observe that we only care about the truth assignments where both assumptions hold. These are the rowns highlighted in green.

Finally, we look at the truth value of the thing to be proved in *only* the green rows. These entries are highlighted in purple. Since they are all T, we can conclude that

whenever p -> q and q -> r, it is also the case that p -> (q ^ r)

[Style note: what is the canonical order of the rows in a truth table for three propositions?]

If we represent the truth value F as 0 and T as 1, we can see that we are simply counting binary integers in the first three columns: 000, 001, 010, 011, 100, …

III. Tautology, satisfiable, contradiction

Which of the following are tautologies? Satisfiable? Unsatisfiable (contradictions)?

1. (p AND q AND r) -> (p OR q)

This is a tautology, so true under any possible assignment of truth values to p, q, and r. Like any tautology, it is necessarily satisfiable but not a contradiction. If you aren't convinced, construct the truth table.

2. ((p -> q) AND (q -> r)) -> (p -> r)

This is also a tautology, so true under any possible assignment of truth values to p, q, and r, and satisfiable, but not a contradiction.

3. (p -> q) -> p

This one isn't a tautology. For it to be true, it's sufficient for p to be true (since anything implies T, but if p is false, p->q is true (regardless of what q is), and then this reduces to T -> F, which is F.

4. (p OR q OR r) AND ((NOT p) OR (NOT q) OR (NOT r)) AND (p OR (NOT q)) AND (q OR (NOT r)) OR (r OR (not p))

Whew, that's ugly. Here's a shorter rewrite. (Same formula, different notation)

$$(p \vee q \vee r) \wedge (\sim p \vee \sim q \vee \sim r) \wedge (p \vee \sim q) \wedge (q \vee \sim r) \wedge (r \vee \sim p)$$

This one is a contradiction, so neither a tautology nor satisfiable. You can see this by writing out the truth table, of course. You can also see it through the following: the first clause says at least one of p, q, r must be true. The second clause says at least one must be false. The final three clauses say that all three must have the same truth value, because they are equivalent to q->p, r->q, and p->r. Those can't all be the case, so this is an unsatisfiable formula. (It's also in CNF – conjunctive normal form – for those who were keeping count.)

5. [challenge/optional] (p <=> (q OR r)) -> ((NOT q) -> (p AND r))**

Rewriting again:

$$(p <-> (q \vee r)) -> (\sim q -> (p \wedge r))$$

This is not easy to see without a truth table, and it's not in a nice neat normal form either. But with some work (e.g., a truth table or some manipulation or some really lucky coin flips) we can see that this is satisfiable but neither a tautology nor a contradiction. For example, the formula is true if p and r are true and q is false. It is false if all three are false.

IV. CNF

Transform the following formula into conjunctive normal form. Show your steps.

p OR (q AND NOT (r AND (s -> t)))

Note that there are many correct answers. Here is one.

a.	p v (q ^ ~(r ^ (s -> t)))	
b.	(p v q) ^ (p v ~(r ^ (s -> t)))	distribute p v
c.	(p v q) ^ (p v (~r v ~(s -> t)))	de Morgan on ~(r ^…)
d.	(p v q) ^ (p v (~r v ~(~s v t)))	definition s -> t
e.	(p v q) ^ (p v (~r v (s v ~t)))	de Morgan on ~(~s v t)
f.	(p v q) ^ (p v ~r v s v ~t))	regrouping (associativity of v)

V. Short certificate

Demonstrate that the formula in problem IV is satisfiable. Explain whether you used a "short certificate" or exhaustive enumeration to make this determination.

Any truth assignment in which p is true satisfies the formula. In particular (and chosen somewhat at random), the truth assignment in which p, q, and r are true and s and t are false satisfies the formula. You can determine that this is true by computing the truth value of the formula under this truth assignment and confirming that the truth assignment satisfies the formula; you don't need to look at other truth assignments to show that it is satisfiable.

[several problems adapted from Ullman FOCS ch12]