THE UNIVERSITY OF MELBOURNE
SCHOOL OF COMPUTING AND INFORMATION SYSTEMS
COMP30026 MODELS OF COMPUTATION

Sample Answers to Tutorial Exercises, Week 6

P6.1 (i) The pair of terms $(h(f(x), g(y, f(x)), y), h(f(u), g(v, v), u))$ is not unifiable. Applying rule 1 (decomposition) to $\{h(f(x), g(y, f(x)), y) = h(f(u), g(v, v), u)\}$, we get

$$\left\{ \begin{array}{rcl} f(x) & = & f(u) \\ g(y, f(x)) & = & g(v, v) \\ y & = & u \end{array} \right\}$$

Applying rule 1 (decomposition) again, to each of the first two equations, yields

$$\left\{ \begin{array}{rcl} x & = & u \\ y & = & v \\ f(x) & = & v \\ y & = & u \end{array} \right\}$$

Applying rule 6 (substitution) with the first equation, we get

$$\left\{ \begin{array}{rcl} x & = & u \\ y & = & v \\ f(u) & = & v \\ y & = & u \end{array} \right\}$$

Applying rule 4 (reorientation) to the third equation, followed by rule 6 to the result yields

$$\left\{ \begin{array}{rcl} x & = & u \\ y & = & f(u) \\ v & = & f(u) \\ y & = & u \end{array} \right\}$$

Applying rule 6 (substitution) with the last equation yields

$$\left\{ \begin{array}{rcl} x & = & u \\ u & = & f(u) \\ v & = & f(u) \\ y & = & u \end{array} \right\}$$

Now the occur check applied to the second equation yields failure.

(ii) The pair of terms $(h(f(g(x, y)), y, g(y, y)), h(f(u), g(a, v), u))$ is unifiable. Applying rule 1 (decomposition) to $\{h(f(g(x, y)), y, g(y, y)) = h(f(u), g(a, v), u)\}$, we get

$$\left\{ \begin{array}{rcl} f(g(x, y)) & = & f(u) \\ y & = & g(a, v) \\ g(y, y) & = & u \end{array} \right\}$$

and a second application yields

$$\left\{\begin{array}{rcl} g(x,y) & = & u \\ y & = & g(a,v) \\ g(y,y) & = & u \end{array}\right\}$$

Applying rule 4 (reorientation) to the first and the third equation, we have

$$\left\{\begin{array}{rcl} u & = & g(x,y) \\ y & = & g(a,v) \\ u & = & g(y,y) \end{array}\right\}$$

Applying rule 6 (to the first equation) we then get

$$\left\{\begin{array}{rcl} u & = & g(x,y) \\ y & = & g(a,v) \\ g(x,y) & = & g(y,y) \end{array}\right\}$$

which, after an application of rule 1 gives

$$\left\{\begin{array}{rcl} u & = & g(x,y) \\ y & = & g(a,v) \\ x & = & y \\ y & = & y \end{array}\right\}$$

The last equation is dropped, by rule 3, and then rule 6 applied to the third equation gives

$$\left\{\begin{array}{rcl} u & = & g(y,y) \\ y & = & g(a,v) \\ x & = & y \end{array}\right\}$$

Finally, rule 6 applied to the second equation gives

$$\left\{\begin{array}{rcl} u & = & g(g(a,v),g(a,v)) \\ y & = & g(a,v) \\ x & = & g(a,v) \end{array}\right\}$$

This is a normal form and $\{u \mapsto g(g(a,v),g(a,v)), y \mapsto g(a,v), x \mapsto g(a,v)\}$ is the most general unifier.

(iii) The pair of terms $(h(g(x,x),g(y,z),g(y,f(z))), h(g(u,v),g(v,u),v))$ is not unifiable. Applying rule 1 (decomposition) to $\{h(g(x,x),g(y,z),g(y,f(z))) = h(g(u,v),g(v,u),v)\}$, we get

$$\left\{\begin{array}{rcl} g(x,x) & = & g(u,v) \\ g(y,z) & = & g(v,u) \\ g(y,f(z)) & = & v \end{array}\right\}$$

Applying rule 1 (decomposition) again, to each of the first two equations, yields

$$\left\{\begin{array}{rcl} x & = & u \\ x & = & v \\ y & = & v \\ z & = & u \\ g(y,f(z)) & = & v \end{array}\right\}$$

Applying rule 4 (reorientation) to the last equation, followed by rule 6 applied to v yields

$$\left\{\begin{array}{lcl} x & = & u \\ x & = & g(y, f(z)) \\ y & = & g(y, f(z)) \\ z & = & u \\ v & = & g(y, f(z)) \end{array}\right\}$$

Now the occur check (rule 5) applied to the third equation yields failure.

(iv) The pair of terms $(h(v, g(v), f(u, a)), h(g(x), y, x))$ is unifiable. Applying rule 1 (decomposition) to $\{h(v, g(v), f(u, a)) = h(g(x), y, x)\}$, we get

$$\left\{\begin{array}{rcl} v & = & g(x) \\ g(v) & = & y \\ f(u, a)) & = & x \end{array}\right\}$$

Reorienting the last two equations:

$$\left\{\begin{array}{lcl} v & = & g(x) \\ y & = & g(v) \\ x & = & f(u, a)) \end{array}\right\}$$

Now replacing x (rule 6):

$$\left\{\begin{array}{lcl} v & = & g(f(u, a)) \\ y & = & g(v) \\ x & = & f(u, a)) \end{array}\right\}$$

Finally replacing v (rule 6):

$$\left\{\begin{array}{lcl} v & = & g(f(u, a)) \\ y & = & g(g(f(u, a))) \\ x & = & f(u, a)) \end{array}\right\}$$

we have a normal form and $\{v \mapsto g(f(u, a)), x \mapsto f(u, a), y \mapsto g(g(f(u, a)))\}$ is the most general unifier.

(v) The pair of terms $(h(f(x, x), y, y, x), h(v, v, f(a, b), a))$ is not unifiable. Applying rule 1 (decomposition) to $\{h(f(x, x), y, y, x) = h(v, v, f(a, b), a)\}$, we get

$$\left\{\begin{array}{rcl} f(x, x) & = & v \\ y & = & v \\ y & = & f(a, b) \\ x & = & a \end{array}\right\}$$

Reorienting the first equation yields

$$\left\{\begin{array}{lcl} v & = & f(x, x) \\ y & = & v \\ y & = & f(a, b) \\ x & = & a \end{array}\right\}$$

Now applying rule 6 to x and then to v, we get

$$\left\{ \begin{array}{rcl} v & = & f(a,a) \\ y & = & f(a,a) \\ y & = & f(a,b) \\ x & = & a \end{array} \right\}$$

Now apply rule 6 to, say, the second equation and get

$$\left\{ \begin{array}{rcl} v & = & f(a,a) \\ y & = & f(a,a) \\ f(a,a) & = & f(a,b) \\ x & = & a \end{array} \right\}$$

Decomposition (rule 1) then yields

$$\left\{ \begin{array}{rcl} v & = & f(a,a) \\ y & = & f(a,a) \\ a & = & a \\ a & = & b \\ x & = & a \end{array} \right\}$$

Now the second-last equation gives match failure (rule 2 applies), and so the original pair of terms were not unifiable.

P6.2 (a) The two statements

S_1:	"No politician is honest."	become	$F_1 \;:\; \forall x\ (\neg P(x) \lor \neg H(x))$
S_2:	"Some politicians are not honest."		$F_2 \;:\; \exists x\ (P(x) \land \neg H(x))$

(b) $F_1 \Rightarrow F_2$ is satisfiable. First let us simplify the formula. Normally it would be a good idea to rename the bound variables, but in this case, it will be preferable to keep the x.

$$\begin{array}{lll} & F_1 \Rightarrow F_2 & \\ \equiv & \forall x\ (\neg P(x) \lor \neg H(x)) \Rightarrow \exists x\ (P(x) \land \neg H(x)) & \text{spell out} \\ \equiv & \neg \forall x\ (\neg P(x) \lor \neg H(x)) \lor \exists x\ (P(x) \land \neg H(x)) & \text{eliminate implication} \\ \equiv & \exists x\ (P(x) \land H(x)) \lor \exists x\ (P(x) \land \neg H(x)) & \text{push negation in} \\ \equiv & \exists x\ ((P(x) \land H(x)) \lor (P(x) \land \neg H(x))) & \exists \text{ distributes over } \lor \\ \equiv & \exists x\ (P(x) \land (H(x) \lor \neg H(x))) & \text{factor out } P(x) \\ \equiv & \exists x\ P(x) & \text{eliminate trivially true conjunct} \end{array}$$

For this formula we can clearly find an interpretation that makes it true. For example, take the domain $\{\mathit{alf}, \mathit{bill}, \mathit{charlie}\}$ and let P and H hold for all elements. Or, take the domain $\mathbb{Z}$, let P stand for "is a prime" and let H stand for "is zero".

(c) $F_1 \Rightarrow F_2$ is not valid. It is easy to find an interpretation that makes $\exists x\ P(x)$ false. For example, take the domain $\{\mathit{alf}, \mathit{bill}, \mathit{charlie}\}$ and let P hold for none of the elements (H can be given any interpretation). Or, take the domain $\mathbb{Z}$, let P stand for "is an even prime greater than 2" and let H stand for "is zero".

(d) The statements

S_3: "No Australian politician is honest."
S_4: "All honest politicians are Australian."

can be expressed

$$S_3: \quad \forall x\ ((A(x) \land P(x)) \Rightarrow \neg H(x))$$
$$S_4: \quad \forall y\ ((P(y) \land H(y)) \Rightarrow A(y))$$

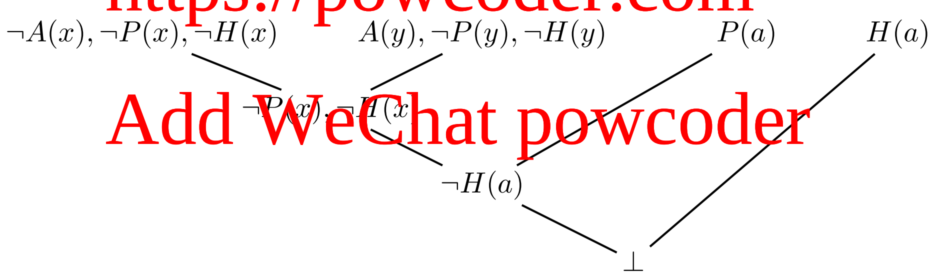
Each of these formulas corresponds to exactly one clause. The clausal forms are:

$$\{\{\neg A(x), \neg H(x), \neg P(x)\}\}$$
$$\{\{A(y), \neg H(y), \neg P(y)\}\}$$

(e) We can show that S_1 is a logical consequence of S_3 and S_4 by refuting $S_3 \land S_4 \land \neg S_1$. So let us write $\neg S_1$ in clausal form (note that we *must* apply the negation *before* "clausifying"; the other way round generally gives an incorrect result):

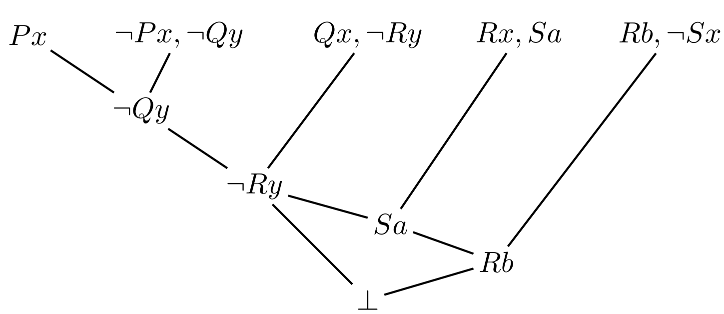
$$\neg \forall x\ (\neg P(x) \lor \neg H(x))$$
$$\exists x\ (P(x) \land H(x)) \qquad \text{push negation in}$$
$$P(a) \land H(a) \qquad \text{Skolemize}$$

Or, written as a set of sets: $\{\{P(a)\}, \{H(a)\}\}$. Added to the other clauses, these allow us to complete the proof by resolution:

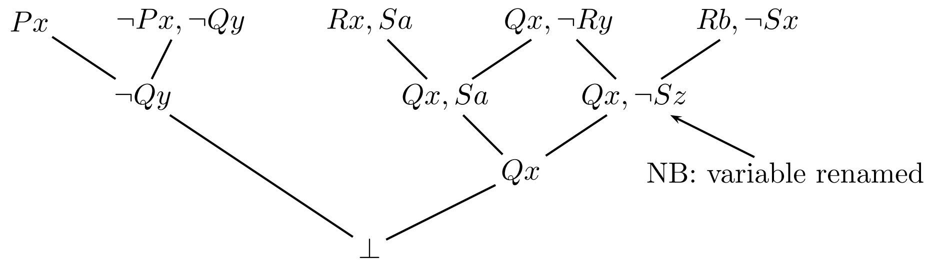


(f) The statement "S_2 is a logical consequence of S_3 and S_4" is false. We can show this by constructing an interpretation which makes S_3 and S_4 true, while making S_2 false. Any interpretation with domain D, in which P is false for all elements of D, will do.

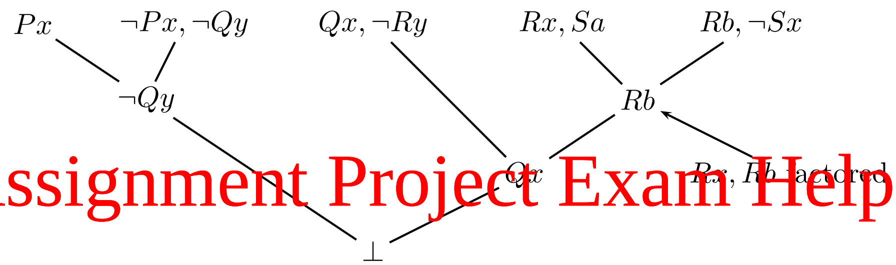
P6.3 (We should rename clauses apart, but in this case, no confusion arises, so we omit that.) We can construct the refutation in 5 resolution steps, that is, the refutation tree has only 5 internal nodes:



Here is another way (5 steps), in which the depth of the refutation tree is somewhat smaller:



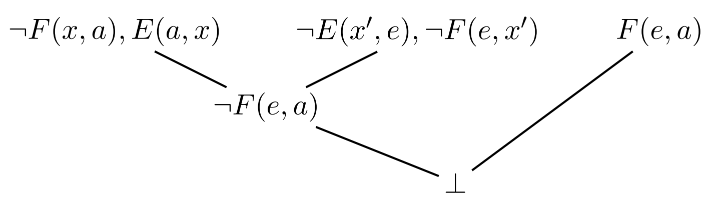
With factoring, we can do it in 4 resolution steps, plus one factoring step:



P6.4 (a) $\forall x\ (F(x,a) \Rightarrow E(a,x))$

(b) $\forall x\ (E(x,e) \Rightarrow \neg F(e,x))$

(c) We capture "Eve is no more fortunate than Adam" as $\neg F(e,a)$. To show that this is a logical consequence of the other two statements, we need to show that every model of $\forall x\ (F(x,a) \Rightarrow E(a,x)) \wedge \forall x\ (E(x,e) \Rightarrow \neg F(e,x))$ makes $F(e,a)$ false. Assume (for contradiction) that there is a model in which $F(e,a)$ is true. Then, by the left conjunct, $E(a,e)$ is also true in this model. But then, by the right conjunct, $\neg F(e,a)$ is also true, that is, $F(e,a)$ is false. But this is a contradiction, so $F(e,a)$ must be false. Indeed a proof by resolution is easy:



P6.8 If you haven't used Haskell to solve this problem, it is not too late!

(a) We can hope to prove an existential claim by brute force, by using Haskell to enumerate candidate witnesses. If a witness appears in a reasonable time we are done. There is no obvious way to refute an existential claim that way, nor to prove a universal claim.

(b) The conjecture is false. The easiest way to get to that conclusion is to write the conjecture as a Haskell expression

```
conjecture k = elem (product (take k primes) + 1) primes
```

(assuming we have defined `primes`) and then check, say: `map conjecture [1..10]` and see what happens. We find that it fails for $k = 6$.

(c) Easy, if we let Haskell do the work:

(3,5), (5,7), (11,13), (17,19), (29,31), (41,43), (59,61), (71,73), (101,103), (107,109), (137,139), (149,151), (179,181), (191,193), (197,199), (227,229), (239,241), (269,271), (281,283), (311,313), (347,349), (419,421), (431,433), (461,463), (521,523), (569,571), (599,601), (617,619), (641,643), (659,661), (809,811), (821,823), (827,829), (857,859), (881,883), (1019,1021), (1031,1033), (1049,1051), (1061,1063), (1091,1093), (1151,1153), (1229,1231), (1277,1279), (1289,1291), (1301,1303), (1319,1321), (1427,1429), (1451,1453), (1481,1483), (1487,1489).

(d) Haskell generates the triple (3,5,7) and then stalls.

(e) ... and for good reason, as there are no other prime triples. However, we can't hope to use Haskell to prove that! Instead we have to think.

Here is why there cannot be any prime triples other than $(3, 5, 7)$. Assume that $p > 3$. Out of p, $p + 2$, and $p + 4$, one must be divisible by 3, and so it is not a prime. The following table shows all the possible remainders of the three numbers, after division by 3:

p	0	1	2
$p+2$	2	0	1
$p+4$	1	2	0

In all cases, one of the three is divisible by 3.

Notice that this proof is not by brute force. Its critical step is to identify an essential property of prime triples and use that, rather than simply enumerate-and-test.